Annual Meeting 2019

Intellectual Property Law Section

January 15, 2019

New York Hilton Midtown

1335 6th Ave, New York, NY 10019

Thank You! This program is made possible by the generous donation of time and expertise by members and volunteers. Thank you to our volunteers—and to you, for choosing NYSBA Programs.

This program is offered for educational purposes. The views and opinions of the faculty expressed during this program are those of the presenters and authors of the materials, including all materials that may have been updated since the books were printed or distributed electronically. Further, the statements made by the faculty during this program do not constitute legal advice.

Accessing the Online Electronic Course Materials

Program materials will be distributed exclusively online in PDF format. It is strongly recommended that you save the course materials in advance, in the event that you will be bringing a computer or tablet with you to the program.

Printing the complete materials is not required for attending the program.

The course materials may be accessed online at:
<< http://www.nysba.org/IPAM19Materials/ >>

A hard copy NotePad will be provided to attendees at the live program site, which contains lined pages for taking notes on each topic, speaker biographies, and presentation slides or outlines if available.

Please note:

- You must have Adobe Acrobat on your computer in order to view, save, and/or print the files. If you do not already have this software, you can download a free copy of Adobe Acrobat Reader at https://get.adobe.com/reader/
- If you are bringing a laptop, tablet or other mobile device with you to the program, please be sure that your batteries are fully charged in advance, as electrical outlets may not be available.
- NYSBA cannot guarantee that free or paid Wi-Fi access will be available for your use at the program location.

MCLE INFORMATION

Program Title: **Intellectual Property Law Section Annual Meeting 2019**
Date: January 15, 2019 Location: New York Hilton Midtown, New York, NY

Evaluation: https://www.nysba.org/am2019-ips0
This evaluation survey link will be emailed to registrants following the program.

Total Credits: **6.5 New York CLE credit hours**

Credit Category:
5.5 Areas of Professional Practice
1.0 Ethics and Professionalism

This course is approved for credit for **both** experienced attorneys and newly admitted attorneys (admitted to the New York Bar for less than two years). Newly admitted attorneys attending via webcast should refer to Additional Information and Policies regarding permitted formats.

Attendance Verification for New York MCLE Credit

In order to receive MCLE credit, attendees must:

1) **Sign in** with registration staff

2) Complete and return a **Verification of Presence form** (included with course materials) at the end of the program or session. For multi-day programs, you will receive a separate form for each day of the program, to be returned each day.

Partial credit for program segments is not allowed. Under New York State Continuing Legal Education Regulations and Guidelines, credit shall be awarded only for attendance at an entire course or program, or for attendance at an entire session of a course or program. Persons who arrive late, depart early, or are absent for any portion of a segment will not receive credit for that segment. The Verification of Presence form certifies presence for the entire presentation. Any exceptions where full educational benefit of the presentation is not received should be indicated on the form and noted with registration personnel.

Program Evaluation

The New York State Bar Association is committed to providing high quality continuing legal education courses, and your feedback regarding speakers and program accommodations is important to us. Following the program, an email will be sent to registrants with a link to complete an online evaluation survey. The link is also listed above.

Additional Information and Policies

Recording of NYSBA seminars, meetings and events is not permitted.

Accredited Provider

The New York State Bar Association's **Section and Meeting Services Department** has been certified by the New York State Continuing Legal Education Board as an accredited provider of continuing legal education courses and programs.

Credit Application Outside of New York State

Attorneys who wish to apply for credit outside of New York State should contact the governing body for MCLE in the respective jurisdiction.

MCLE Certificates

MCLE Certificates will be emailed to attendees a few weeks after the program, or mailed to those without an email address on file. **To update your contact information with NYSBA**, visit www.nysba.org/MyProfile, or contact the Member Resource Center at (800) 582-2452 or MRC@nysba.org.

Newly Admitted Attorneys—Permitted Formats

In accordance with New York CLE Board Regulations and Guidelines (section 2, part C), newly admitted attorneys (admitted to the New York Bar for less than two years) must complete **Skills** credit in the traditional live classroom setting or by fully interactive videoconference. **Ethics and Professionalism** credit may be completed in the traditional live classroom setting; by fully interactive videoconference; or by simultaneous transmission with synchronous interactivity, such as a live-streamed webcast that allows questions during the program. **Law Practice Management** and **Areas of Professional Practice** credit may be completed in any approved format.

Tuition Assistance

New York State Bar Association members and non-members may apply for a discount or scholarship to attend MCLE programs, based on financial hardship. This discount applies to the educational portion of the program only. Application details can be found at www.nysba.org/SectionCLEAssistance.

Questions

For questions, contact the NYSBA Section and Meeting Services Department at SectionCLE@nysba.org, or (800) 582-2452 (or (518) 463-3724 in the Albany area).

NEW YORK STATE BAR ASSOCIATION

ANNUAL MEETING 2019

Intellectual Property Law Section

Tuesday, January 15, 2019 | 8:45 a.m. – 5:00 p.m.
New York Hilton Midtown | Mercury Ballroom, Third Floor

6.5 Credits
5.5 Areas of Professional Practice | 1.0 Ethics
This program is transitional and is suitable for all attorneys including those newly admitted.

Lunch
12:50 p.m. – 1:45 p.m.

Offsite Reception

5:45 p.m. – 8:30 p.m. | Bill's Bar & Burger Rockefeller Center
16 W 51st St, New York, NY 10019

MCLE Program
8:45 a.m. – 5:00 p.m. | New York Hilton Midtown | Mercury Ballroom, Third Floor

Agenda

8:45 a.m. Registration and Continental Breakfast - Sponsored by Davis & Gilbert LLP

8:55 a.m. – 9:10 a.m. **Welcoming Remarks**
Chair/Program Chair

9:10 a.m. – 10:00 a.m. **Ethical Issues in Your New Media Practice**

The ethical obligations of outside counsel in advising clients with respect to emerging social media. A discussion on evolving ethical rules and best practices for attorneys in social media, as well as emerging liability concerns and predictions.

Speakers:
Anthony LoCicero, Esq., Amster Rothstein
Theo Nittis, Principal, Gemini Risk Partners, LLC
John Reed, Marketing Consultant, RainBDM
Richard Searle Eisert, Esq., Davis & Gilbert

(1.0 Credit in Ethics)

10:00 a.m. – 10:15 a.m. Break - Sponsored by Golenbock Eiseman Assor Bell & Peskoe LLP

10:15 a.m. – 11:30 a.m. **Entertainment and New Media**

Hollywood stars, sports teams and leagues are prolific trademark and copyright/media rights holders. The rise of new media platforms and formats is accompanied by new IP protection challenges, e.g., clearance, enforcement, monitoring, obtaining rights.

Speakers:
Danielle E. Maggiacomo, Esq., Frankfurt Kurnit (Moderator)
Catherine Farrelly, Esq., Frankfurt Kurnit
Jemar Daniel, Esq., Sr. Vice President and Senior Counsel, Business Legal Affairs, Viacom
Deborah Robinson, Esq., VP & Sr. Counsel Anti-Piracy, Viacom
Adrian D. Stubbs, Esq., Assistant General Counsel, CBS Television
Matthew Winterroth, Esq., VP & Intellectual Property Counsel, WWE

(1.5 Credits in Areas of Professional Practice)

11:30 a.m. – 11:45 a.m. Break - Sponsored by Kilpatrick Townsend & Stockton LLP

11:45 a.m. – 12:35 p.m. **Advertising, Social Media and the FTC**

Impact on how the FTC is changing the way brand owners market in the various new media channels, e.g., influencers, claim substantiation, etc.

Speakers: **Barry Benjamin, Esq.**, Kilpatrick Townsend LLP
Nur-ul Haq, Esq., VP & Counsel, Tech & Kids Compliance, Viacom
Ann Gorfinkle, Esq., VP, Standards and Practices for Nickelodeon, Viacom
Rebecca Leigh Griffith Esq., Senior Counsel, Unilever United States, Inc.
(1.0 Credit in Areas of Professional Practice)

12:50 p.m. – 1:45 p.m. Lunch

2:00 p.m. – 2:50 p.m. **The Media-Content Deal**

Do's and Don'ts for Parties to a New Media Deal. The panel will take us through the important aspects of a typical deal between companies like Amazon and Content Providers.

Speakers: **Marc Lieberstein, Esq.**, Kilpatrick Townsend, LLP (Moderator)
David Stonehill, Esq., SVP & Deputy General Counsel, Global Digital & New Media, Viacom
Rick Baker, Esq., SVP & Deputy General Counsel, Content Distribution, Viacom
Jill Greenwald, Esq., Assistant Chief Counsel, ABC, Inc.
(1.0 Credit in Areas of Professional Practice)

2:50 p.m. – 3:00 p.m. Break - Sponsored by Golenbock Eiseman Assor Bell & Peskoe LLP

3:00 p.m. – 3:50 p.m. **Privacy and the Internet of Things (IoT)**

The IoT is now in our homes, on the streets, and on your person as new smart appliances, city-sensors, and wearable tech. This rise of "smart" devices in our homes and on our person, has raised significant and growing data privacy concerns related not only to social media, but also the devices we use to stay connected with the world.

This privacy focused panel will discuss the GDPR and upcoming U.S. state data privacy laws (e.g., California Consumer Privacy Act, A.B. 375). How privacy and consumer protection laws intersect with the rise of ever present IoT "smart devices" in our homes or on our person, including data gathering, storage, and use issues for devices like Alexa, Cortana, smart TV's, smart watches.

Speakers: **Leonie Huang, Esq.**, Holland & Knight (Moderator)
Mark Melodia, Esq., Partner, Holland & Knight
Jessica Lee, Esq., Partner, Loeb & Loeb
Anthony Ford, Esq., Senior Data Privacy Counsel, Medidata Solutions, Inc.
Manas Mohapatra, Esq., Chief Privacy Officer at Viacom
(1.0 Credit in Areas of Professional Practice)

3:50 p.m. – 4:10 p.m. Break - Sponsored by Barclay Damon

4:10 p.m. – 5:00 p.m. **Patents in the New Media**

A discussion on patents covering new media technology and understanding patent opportunities and pitfalls with content delivery.

Speakers: **Douglas A. Miro, Esq.**, Amster Rothstein & Ebenstein, LLP (Moderator)
Charles Macedo, Esq., Amster Rothstein & Ebenstein, LLP
Richard P. Zemsky, Chief Operating Officer, AIMeCast, LLC
(1.0 Credit in Areas of Professional Practice)

5:45 p.m. – 8:30 p.m. **Off-Site Reception** - Sponsored by Compumark
Bill's Bar & Burger Rockefeller Center
16 W 51st St, New York, NY 10019

SECTION CHAIR
Robin Silverman, Esq. | Golenbock Eiseman Assor Bell & Peskoe LLP | New York

PROGRAM CHAIRS
Marc A. Lieberstein, Esq. | Kilpatrick Townsend & Stockton LLP | New York
Leonie Huang, Esq. | Holland & Knight LLP | New York
Doug A. Miro, Esq. | Amster, Rothstein & Ebenstein LLP | Bellmore

Lawyer Assistance Program 800.255.0569

Q. What is LAP?

A. The Lawyer Assistance Program is a program of the New York State Bar Association established to help attorneys, judges, and law students in New York State (NYSBA members and non-members) who are affected by alcoholism, drug abuse, gambling, depression, other mental health issues, or debilitating stress.

Q. What services does LAP provide?

A. Services are **free** and include:

- Early identification of impairment
- Intervention and motivation to seek help
- Assessment, evaluation and development of an appropriate treatment plan
- Referral to community resources, self-help groups, inpatient treatment, outpatient counseling, and rehabilitation services
- Referral to a trained peer assistant – attorneys who have faced their own difficulties and volunteer to assist a struggling colleague by providing support, understanding, guidance, and good listening
- Information and consultation for those (family, firm, and judges) concerned about an attorney
- Training programs on recognizing, preventing, and dealing with addiction, stress, depression, and other mental health issues

Q. Are LAP services confidential?

A. Absolutely, this wouldn't work any other way. In fact your confidentiality is guaranteed and protected under Section 499 of the Judiciary Law. Confidentiality is the hallmark of the program and the reason it has remained viable for almost 20 years.

Judiciary Law Section 499 Lawyer Assistance Committees Chapter 327 of the Laws of 1993

Confidential information privileged. The confidential relations and communications between a member or authorized agent of a lawyer assistance committee sponsored by a state or local bar association and any person, firm or corporation communicating with such a committee, its members or authorized agents shall be deemed to be privileged on the same basis as those provided by law between attorney and client. Such privileges may be waived only by the person, firm or corporation who has furnished information to the committee.

Q. How do I access LAP services?

A. LAP services are accessed voluntarily by calling **800.255.0569** or connecting to our website **www.nysba.org/lap**

Q. What can I expect when I contact LAP?

A. You can expect to speak to a Lawyer Assistance professional who has extensive experience with the issues and with the lawyer population. You can expect the undivided attention you deserve to share what's on your mind and to explore options for addressing your concerns. You will receive referrals, suggestions, and support. The LAP professional will ask your permission to check in with you in the weeks following your initial call to the LAP office.

Q. Can I expect resolution of my problem?

A. The LAP instills hope through the peer assistant volunteers, many of whom have triumphed over their own significant personal problems. Also there is evidence that appropriate treatment and support is effective in most cases of mental health problems. For example, a combination of medication and therapy effectively treats depression in 85% of the cases.

Personal Inventory

Personal problems such as alcoholism, substance abuse, depression and stress affect one's ability to practice law. Take time to review the following questions and consider whether you or a colleague would benefit from the available Lawyer Assistance Program services. If you answer "yes" to any of these questions, you may need help.

1. **Are my associates, clients or family saying that my behavior has changed or that I don't seem myself?**
2. **Is it difficult for me to maintain a routine and stay on top of responsibilities?**
3. **Have I experienced memory problems or an inability to concentrate?**
4. **Am I having difficulty managing emotions such as anger and sadness?**
5. **Have I missed appointments or appearances or failed to return phone calls? Am I keeping up with correspondence?**
6. **Have my sleeping and eating habits changed?**
7. **Am I experiencing a pattern of relationship problems with significant people in my life (spouse/parent, children, partners/associates)?**
8. **Does my family have a history of alcoholism, substance abuse or depression?**
9. **Do I drink or take drugs to deal with my problems?**
10. **In the last few months, have I had more drinks or drugs than I intended, or felt that I should cut back or quit, but could not?**
11. **Is gambling making me careless of my financial responsibilities?**
12. **Do I feel so stressed, burned out and depressed that I have thoughts of suicide?**

There Is Hope

CONTACT LAP TODAY FOR FREE CONFIDENTIAL ASSISTANCE AND SUPPORT

The sooner the better!

1.800.255.0569

NEW YORK STATE BAR ASSOCIATION

☐ As a NYSBA member, **PLEASE BILL ME $30 for Intellectual Property Law Section dues.** (law student rate is $15)

☐ I wish to become a member of the NYSBA (please see Association membership dues categories) and the Intellectual Property Law Section. **PLEASE BILL ME for both.**

☐ I am a Section member — please consider me for appointment to committees marked.

Name _____

Address _____

_____

City _____ State _____ Zip _____

The above address is my ☐ Home ☐ Office ☐ Both

Please supply us with an additional address.

Name _____

Address _____

City _____ State _____ Zip _____

Office phone (_____) _____

Home phone (_____) _____

Fax number (_____) _____

E-mail address _____

Date of birth _____ /_____ /_____

Law school _____

Graduation date _____

States and dates of admission to Bar: _____

Intellectual Property Law Section Committees

Please designate from the list below, those committees in which you wish to participate. For a list of committee chairs and their email addresses, visit the executive committee roster on our web-site at www.nysba.org/ipl

___ Advertising Law (IPS3000)
___ Copyright Law (IPS1100)
___ Cyber Security and Data Privacy (IPS3200)
___ Diversity Initiative (IPS2400)
___ Ethics (IPS2600)
___ In-House Initiative (IPS2900)
___ International Intellectual Property Law (IPS2200)
___ Internet and Technology Law (IPS1800)
___ Legislative/Amicus (IPS2300)
___ Litigation (IPS2500)
___ Membership (IPS1040)
___ Patent Law (IPS1300)
___ Pro Bono and Public Interest (IPS2700)
___ Trademark Law (IPS1600)
___ Trade Secrets (IPS1500)
___ Transactional Law (IPS1400)
___ Website Task Force (IPS3100)
___ Young Lawyers (IPS1700)

JOIN OUR SECTION

2019 ANNUAL MEMBERSHIP DUES

Class based on first year of admission to bar of any state. Membership year runs January through December.

ACTIVE/ASSOCIATE IN-STATE ATTORNEY MEMBERSHIP	
Attorneys admitted 2011 and prior	$275
Attorneys admitted 2012-2013	185
Attorneys admitted 2014-2015	125
Attorneys admitted 2016 - 3.31.2018	60
ACTIVE/ASSOCIATE OUT-OF-STATE ATTORNEY MEMBERSHIP	
Attorneys admitted 2011 and prior	$180
Attorneys admitted 2012-2013	150
Attorneys admitted 2014-2015	120
Attorneys admitted 2016 - 3.31.2018	60
OTHER	
Sustaining Member	$400
Affiliate Member	185
Newly Admitted Member*	FREE

DEFINITIONS

Active In-State = Attorneys admitted in NYS, who work and/or reside in NYS
Associate In-State = Attorneys not admitted in NYS, who work and/or reside in NYS
Active Out-of-State = Attorneys admitted in NYS, who neither work nor reside in NYS
Associate Out-of-State = Attorneys not admitted in NYS, who neither work nor reside in NYS
Sustaining = Attorney members who voluntarily provide additional funds to further support the work of the Association
Affiliate = Person(s) holding a JD, not admitted to practice, who work for a law school or bar association
*Newly admitted = Attorneys admitted on or after April 1, 2018

Please return this application to:

MEMBER RESOURCE CENTER,
New York State Bar Association, One Elk Street, Albany NY 12207
Phone 800.582.2452/518.463.3200 • FAX 518.463.5993
E-mail mrc@nysba.org • www.nysba.org

TABLE OF CONTENTS

Ethical Issues in Your New Media Practice

Anthony LoCicero, Esq.
Amster Rothstein

Theo Nittis, Principal
Gemini Risk Partners, LLC

John Reed
Marketing Consultant, RainBDM

Richard Searle Eisert, Esq.
Davis & Gilbert

Ethical Issues In Your New Media Practice

Anthony F. Lo Cicero, Esq., Partner
AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Theodore Nittis, Esq.
Principal
GEMINI RISK PARTNERS

John F. Reed, Esq.,
Founder/Chief Consultant
RAIN BDM
Business Development and Marketing for Law Firms

NYSBA Annual Meeting 2019
January 14-18
9:00 am

DISCLAIMER

The following presentation reflects the personal opinions of its authors and does not necessarily represent the views of their respective employers or of the NYSBA. Additionally, the following content is presented solely for the purposes of discussion and illustration, and does not comprise, nor is not to be considered, as legal advice.

Competence

- RULE 1.1: COMPETENCE (a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
- Comment 8:To maintain the requisite knowledge and skill, a lawyer should . . . keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information. . . .

Material Developments

- RULE 1.4: COMMUNICATION (a) A lawyer shall: (1) promptly inform the client of . . . material developments in the matter . . .
- Do data breaches constitute “material developments”?

Unauthorized Disclosure

- RULE 1.6: CONFIDENTIALITY OF INFORMATION: (c) A lawyer [shall] make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

Safeguarding Confidential Information

- Comment 16:Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule, or may give informed consent to forgo security measures that would otherwise be required by this Rule. . . .

Safeguarding Confidential Information

- Comment 17: . . However, a lawyer may be required to take specific steps to safeguard a client's information to comply with a court order (such as a protective order) or to comply with other law (such as state and federal laws or court rules that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information. . . .

Publicity

- RULE 3.6:TRIAL PUBLICITY:(a) A lawyer who is participating in or has participated in a criminal or civil matter shall not make an extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.

Advertising

- RULE 7.1:ADVERTISING: (a) A lawyer or law firm shall not use or disseminate or participate in the use or
- dissemination of any advertisement that:
- (1) contains statements or claims that are false, deceptive or misleading; or (2) violates a Rule.

Advertising and New Media Issues

- Which state rules govern new media advertising which can be viewed anywhere?
- Do new media communications (like blogs or tweets) create an attorney-client relationship?
- Does accepting a Linked- in endorsement constitute attorney advertising?
- Etc?

Entertainment and New Media

Danielle E. Maggiacomo, Esq.
Frankfurt Kurnit (Moderator)

Catherine Farrelly, Esq.
Frankfurt Kurnit

Jemar Daniel, Esq.
Vice President and Senior Counsel, Viacom

Deborah Robinson, Esq.
VP & Sr. Counsel Anti-Piracy, Viacom

Adrian D. Stubbs, Esq.
Assistant General Counsel, CBS Television

Matthew Winterroth, Esq.
VP & Intellectual Property Counsel, WWE

SAMPLE TALENT AGREEMENT

As of [INSERT DATE]

[TALENT NAME]
[TALENT ADDRESS]

Dear [INSERT NAME]:

This letter sets forth the terms of the agreement between [INSERT NAME] ("You") and [NETWORK] ("Producer") for your services with respect to the production of certain programming, and related activities for Producer (the "Agreement").

1. Engagement
   (a) Producer hereby engages You during the Term (defined below), and You accept such engagement and agree to furnish all artistic and professional services customarily rendered by hosts, analysts, reporters, and other on-camera talent, and in related capacities, in connection with such sports and entertainment programming as Producer may assign, at any time during the Term of the Agreement, for use in connection with any media coverage, including but not limited to television or Internet coverage, produced or controlled by or on behalf of Producer and/or its affiliates (each, a "Program", collectively, the "Programs").
   (b) In addition, upon Producer's reasonable request, You shall be available for the following: development meetings and media days; videotaping and/or voicing of promotional spots, interstitial materials and sales and marketing materials; on-campus promotional appearances in conjunction with any events You cover; and a reasonable number of interviews (whether via radio, podcasting, print, television, etc.). Further, upon Producer's request, You shall provide regular written contributions to Producer's affiliated websites.
   (c) You shall perform your services on such dates, at such places, at such times, and on such Programs as Producer assigns. Producer shall have full discretion as to your assignments. Your duties to Producer take priority over all other permitted professional and personal commitments. Your services shall be performed competently and efficiently and subject to the reasonable creative direction of Producer.

2. Term
   The term begins as of [INSERT DATE] and continues through and includes [INSERT DATE] (the "Term").

3. Compensation
   (a) In consideration of providing your services and the rights granted hereunder, Producer shall pay You as follows during the Term: [INSERT RATE]. Producer shall make applicable withholdings and deductions as required by law.
   (b) You represent and warrant that You are and will remain at all times during the Term: (i) a citizen or national of the United States; or (ii) an alien lawfully admitted in the United States for permanent residence; or (iii) an alien authorized by the United States Immigration and Naturalization Service to work in the United States. You further represent and warrant that You have completed, executed and delivered to Producer Form I-9, all in compliance with the Immigration Reform and Control Act of 1986. Any breach of this subparagraph is a material breach of this agreement.
   (c) In connection with your services hereunder, Producer may provide You with round-trip coach transportation, accommodations, or reimbursement for travel expenses, as applicable, in accordance with Producer's then current travel policy.

4. Work-For-Hire
   You acknowledge that your services hereunder and the results and proceeds thereof, including any contributions to Producer's affiliated websites (collectively, the "Materials"), have been specially ordered as part of a multimedia program and shall hereinafter be deemed a work-made-for-hire for Producer. As between You and Producer, Producer shall own all right, title and interest in and to the Materials, including but not limited to the copyright therein, and shall have the right to distribute and exhibit them in all media now known or hereafter created (including but not limited to standard and nonstandard television, video on demand, home video, DVD, wireless, broadband, Internet, print, satellite and over-the-air radio, etc.) by any means transmitted, throughout the world in perpetuity without any further payment to You. You hereby

waive any “moral” or other rights of authorship (droit moral) which may accrue or have accrued to You under any laws of any jurisdiction, including, without limitation, any right to publish or withhold publication, to be or not to be associated with the Programs or to preserve the integrity of the Programs. If for any reason the Materials or any portion thereof are not deemed works-made-for-hire, then this contract will be deemed an irrevocable assignment to Producer of all rights, including but not limited to the copyright, therein. You agree to execute all documents reasonably necessary to evidence the foregoing. If You fail to do so on a timely basis, then You hereby appoint Producer as your attorney-in-fact to execute such documents; such appointment shall be deemed irrevocable and coupled with an interest. Without limiting the generality of the foregoing, Producer and any designee of Producer shall have the exclusive, perpetual and worldwide right to reproduce, edit, change, alter, add to, take from, manufacture, sell, distribute, advertise, license, or publicly perform, in any medium now known or hereafter devised, and/or otherwise exploit the Materials and the Programs, and other reproductions embodying the Materials and the Programs, under any trademarks, or trade names, and to lease, license, convey or otherwise use or dispose of any Materials and/or Programs, by any method, or in any field of use, now or hereafter known, on any terms Producer approves, or Producer may refrain from doing any of the foregoing in its sole and absolute discretion.

5. Promotional Rights
   Producer, any sponsor of the Programs, any such sponsor’s advertising agency, any distributor of the Programs, and any licensee of Producer, shall have the right, and may grant others the right, to use, in any medium, your name, voice, picture, approved likeness, approved biography, and other identifying attributes of You, as well as portions of the Materials and the Programs, as news information, for the purposes of trade, or for advertising purposes, including but not limited to “institutional” advertising and including but not limited to the advertising, promotion or exhibition of the Materials, the Programs, and/or Producer.

6. Exclusivity
   Your services during the Term are exclusive to Producer in all forms of media now known or hereafter created, including but not limited to standard and nonstandard television, video on demand, home video, DVD, wireless, broadband and Internet, print, satellite and over-the-air radio, etc. Without Producer’s prior written approval, You shall not perform any media services for, or permit the use of your name, likeness, voice or endorsement by, any person, firm or corporation or on your own account. You shall not engage in any activity of any kind that interferes or conflicts with the performance of your services hereunder or with the rights granted herein.

7. Force Majeure
   In the event that, because of: an act of God; inevitable accident; fire; lockout, strike or other labor dispute; riot or civil commotion; act of public enemy; enactment, rule, order or act of government or governmental instrumentality (whether federal, state, local or foreign); failure of technical facilities; failure or delay of transportation facilities; or other cause of similar or different nature beyond Producer’s control, the normal telecast and/or program production of Producer is prevented and/or suspended, Producer may suspend the performance of your services and the payment of compensation hereunder during the continuation of such prevention or suspension, and, at its election, may extend the Term for the number of days equal to the number of days of such suspension.

8. Termination Rights
   (a) Producer may terminate this Agreement at any time upon five (5) days written notice to You for any reason or no reason (other than those set forth in subparagraph (b) below which shall be governed by that subparagraph). In such case, Producer shall pay You for all work performed up to the date of termination.
   (b) In addition, Producer may, at any time, upon written notice to You, terminate this Agreement or suspend, withhold and/or reduce compensation hereunder, if: (1) You breach your material obligations hereunder, which breach, if capable of cure, remains uncured for a period of five (5) days following your receipt of Producer’s written notice thereof; (2) You commit any willful or egregious action which would constitute an act of moral turpitude or which would otherwise constitute public humiliation to Producer; (3) You are arrested or charged in connection with embezzlement, fraud or any other crime; or (4) in Producer’s judgment, You are unable to or have failed to fully perform the services required of You. Without limitation, “failure to perform” shall include: (i) inadequate preparation for or lack of punctuality

in attending scheduled work sessions, tapings and live telecasts and rehearsals or preparation therefor; (ii) intentional or continual activities (whether by commission or omission) contrary to the instructions of Producer's President or his delegate; and (iii) your "incapacity," which shall mean any material physical, mental or other disability which renders You incapable of fully performing all services required to be performed by You, or any material physical alteration or change of your facial or physical appearance or any material impairment of your voice. If Producer terminates this Agreement in accordance with this paragraph 8, it shall be under no further obligation to You except to pay You for all work performed by You up to the date of termination. Any termination by Producer hereunder will not be deemed a waiver of any other rights that Producer may have.

11. FCC Regulations
Reference is hereby made to Section 507 of the Federal Communications Act which makes it a criminal offense for any person to accept or pay, or agree to accept or pay, any money, services or other valuable consideration for the inclusion of any material or play as part of a television program without disclosing the fact of such payment or agreement. You acknowledge that You are familiar with the requirements of the Act and agree that You will not accept, pay or agree to accept or pay any money or other valuable consideration, other than the compensation payable hereunder, for the inclusion of any material or plug as part of the Materials.

12. Representations and Warranties
You represent and warrant that: (i) You have no existing endorsement, sponsorship or similar agreements concerning your services or name or likeness, and You shall not enter into any such endorsement, sponsorship or similar agreement during the Term of this Agreement; (ii) except for any material Producer provides to You, the Materials (including, without limitation, all ideas or materials of any nature which You furnish hereunder) will be your sole original creation and will not, that You know of or with reasonable diligence could discover, violate or infringe any rights of any third party, including without limitation, a defamation, libel, slander or violation of any right of privacy or publicity; (iii) You have the full right, power and authority to enter into and completely perform your obligations hereunder and to grant all rights granted herein; and (iv) there are no rights or commitments of any nature outstanding in favor of any person, firm or corporation that would or might impair, interfere with or infringe upon the rights herein granted and You have obtained or will obtain all required permission or grants of authority necessary with respect to your obligations hereunder.

13. Indemnification
You shall indemnify, defend and hold harmless Producer, Producer's parent, subsidiaries and affiliated entities and their respective officers, directors, employees and agents, sponsors and advertising agencies, any stations or systems over which the Programs are telecast and/or exhibited and any licensee of Producer from and against any and all claims, damages, liabilities, costs and expenses, including reasonable counsel fees, arising out of: (i) the use of any material or services furnished by You in connection with the telecast and/or exhibition of the Programs unless specifically approved by Producer; (ii) any acts done or words spoken by You, unless such acts or words have been specifically supplied or approved by Producer; and (iii) any breach by You of any warranty, representation or agreement made by You herein.

14. Confidentiality
In connection with your engagement hereunder by Producer, Producer anticipates that You may be provided with or exposed to certain non-public information concerning Producer, its affiliates, assigns or licensees, which information, together with notes, analyses, compilations, studies or other documents prepared by Producer based upon, containing or otherwise reflecting such information, is hereinafter referred to as the "Confidential Information." You shall, except to the extent permitted below, keep such Confidential Information strictly confidential in perpetuity. As such, You shall not, during the Term or any time thereafter, use for your own purposes, or disclose to or for the benefit of any third party, any trade secret or other Confidential Information of Producer, its affiliates to a third party (except as may be required by law or in the performance of your duties hereunder consistent with their respective policies) and shall comply with any confidentiality obligations of Producer, its affiliates, whether under agreement or (to the extent known to You) otherwise. All Confidential Information disclosed by Producer and its affiliates is and

shall remain the property of Producer or its affiliates, as applicable. Notwithstanding the foregoing, Confidential Information does not include information which: (i) is or becomes generally available to the public other than as a result of a disclosure by You or any other person who directly or indirectly receives such information from You or at your direction; or (ii) is or becomes available to You on a nonconfidential basis from a source which is entitled to disclose it to You. Further, You and your respective agents agree that the specific terms and conditions of this Agreement are confidential, and, therefore, shall not, except as may be necessary to comply with any applicable law, be made available to third parties without the prior written consent of Producer. You agree that You shall cause your agents to comply with this confidentiality provision in the same manner as if they have signed this Agreement.

15. Miscellaneous

(a) You acknowledge that your services are of a special, unique, extraordinary and intellectual character, which gives them peculiar value, and that a breach of any provision may cause irreparable injury to Producer, which may not be adequately or reasonably compensated in damages in an action at law. Therefore, You agree that Producer may seek injunctive relief to prevent such breach in addition to all other rights or remedies it may have.

(b) This Agreement may be assigned by Producer to any company controlling, under common control with or controlled by Producer, or which assumes the assets or operations of Producer, provided that Producer shall remain liable for its obligations hereunder unless such assignment is in writing and the assignee assumes all of Producer's obligations hereunder. This Agreement may not be assigned by You.

(c) All notices required to be given hereunder shall be given in writing, by personal delivery or by certified mail, return receipt requested, by overnight courier, signature required, or by facsimile with verification of receipt, at the respective addresses of the parties hereto set forth above, or at such other address as may be designed in writing by either party, and, in the case of Producer, to the attention of its Executive Vice President and General Counsel. Any notice given by mail shall be deemed to have been received on the date of actual receipt as evidenced by signature or other proof of delivery.

(e) This Agreement shall constitute the entire understanding between the parties with respect to its subject matter and shall supersede any and all prior agreements and understandings between the parties with respect to the subject matter. This Agreement may not be modified, altered, or amended except in writing signed by both parties.

(f) This Agreement has been entered into in the [INSERT STATE] and shall be governed by [INSERT JURISDICTION] law applicable to contracts executed and performed entirely therein (without regard to the conflicts of law principles).

PROGRAMMING AGREEMENT

1. Event. The "Event" is [INCLUDE DESCRIPTION OF EVENT].

2. Licensed Territory. The [INSERT TERRITORY] (the "Licensed Territory").

3. Term. The term begins on the [INSERT DATE] and continues in full force and effect through [INSERT DATE] (the "Term").

4. Programs. Licensor shall produce and deliver to Licensee [INSERT NUMBER OF PROGRAMS] fully-produced thirty (30) minute programs of the Event (each, a "Program" and collectively, the "Programs"), each formatted in [INSERT NUMBER OF SEGMENTS] segments totaling [INSERT MINUTES] minutes of content per Program, closed captioning, and formatted for commercial breaks as directed by Licensee. Licensee may add any of its own elements to the Programs, such as lead-ins, intros and similar elements (collectively, the "Licensee Materials") at its own expense and discretion.

5. Grant of Rights. Licensor hereby grants Licensee the following irrevocable rights during the Term:
   a. Telecast Rights. With respect to each Program, Licensor grants to Licensee an irrevocable, perpetual, right and license to telecast, exhibit, distribute and license for transmission and exhibition the Programs, and any material included in the Programs, in any and all media, technology and distribution methods, including over any form of television, interactive and online media (whether currently in existence or hereafter developed) (all such rights collectively referred to as the right to "Telecast").

   b. Exclusivity. Licensee's rights in and to the Event and the Programs are exclusive. Licensor has not and will not grant to any third-party any of the rights granted to Licensee hereunder, including, but not limited to, the right to Telecast any part of the Event and the Programs.

   c. Excerpt Rights. During the Term and thereafter in perpetuity, Licensee may Telecast excerpts of each Program in new programming and in connection with advertising, marketing, sales, research, and promotion of the Programs and/or the Network.

6. Licensee Graphics. Licensee shall provide Licensor with a complete graphics package (the "Licensee Graphics") for use in the Programs. Licensor has no other right in and to the Licensee Graphics. Licensor acknowledges and agrees that it shall not combine any other graphic elements with the Licensee Graphics, shall not alter the Licensee Graphics in any manner, including proportions, font, design, arrangement, colors or elements nor may it morph or otherwise distort the Licensee Graphics in perspective or appearance. Licensor further acknowledges and agrees that the Licensee Graphics and/or any portion thereof may not be used in any offensive, vulgar, sexually explicit, obscene, defamatory or otherwise objectionable manner, as determined by Licensee in its sole discretion

7. Copyright. Licensor at all times and in perpetuity owns all right, title, and interest, including, but not limited to, all copyrights, in and to the Programs.

8. Payment Obligations. In consideration of the rights and licenses granted to Licensor hereunder, Licensor shall pay to Licensee the total amount of [INSERT FIGURE], as follows: [INSERT PAYMENT SCHEDULE]

9. Exhibitions and Scheduling. Licensee has the right to an unlimited number of Telecasts of each Program on [NETWORK] (the "Network"), and the elements thereof in perpetuity, at dates and times scheduled by Licensee within its sole discretion. Notwithstanding the foregoing, Licensee

acknowledges and agrees that it shall air each Program on the Network at least [INSERT NUMBER] during the Term (each, a "Guaranteed Telecast," together, the "Guaranteed Telecasts") on specific day and time slots to be determined by Licensee in its sole discretion.

10. Production and Deliverables. In addition to Licensor's obligations otherwise set forth in this Agreement, Licensor shall do the following at its sole cost and expense:
    a. Provide the fully-produced Programs (in accordance with Section 4 above) to Licensee [INSERT DELIVERY INSTRUCTIONS]
    b. Consult with Licensee regarding talent, with all talent subject to Licensee's approval;
    c. Clear all elements included within each Program for Telecast by Licensee as set forth herein, including, but not limited to, the rights to use the names, voices and likenesses of the participants, as well as any logos of any sponsor and any branding appearing in the Programs, and any music included in the Programs; and
    d. Secure and deliver to Licensee music cue sheets for any music used in the Programs, and signed releases and/or licenses with respect to any footage and/or photos used in the Programs.

11. Sponsorships/Sponsor Enhancements/Billboards/Commercial Inventory.
    a. Sponsorships. Licensor has the exclusive right to sell the title sponsorship to the Program. Licensee has the exclusive right to sell the presenting sponsorship to the Program.

    b. Sponsor Enhancements. In each Program, Licensee shall provide Licensor with [INSERT NUMBER] of the in-program sponsored elements for use by the designated sponsors of the Event. Each sponsored element supplied by Licensor is subject to Licensee's standards and practices ("Licensee's Standards and Practices") and Licensee's prior approval. Licensee retains the unfettered right to sell separately or packaged with commercial inventory all remaining in-program sponsored elements in each Program.

    c. Billboards. In each Program, Licensee shall provide Licensor with [INSERT NUMBER] of the in-program billboards for use by the designated sponsors of the Event. Each billboard position will include a graphic and an on-air read. Each billboard position supplied by Licensor is subject to Licensee's Standards and Practices and Licensee's prior approval.

    d. Commercial Inventory. Licensee shall provide Licensor with [INSERT NUMBER] thirty (30) second units of commercial inventory in each Guaranteed Telecast of each Program. Licensee retains all remaining commercial and promotional inventory in each Telecast of each Program. Licensor's commercial inventory within the Programs is to be used for the Event designated sponsors. Each party retains the proceeds from its sale of such inventory, provided, however, that all commercial units supplied by Licensor are subject to Licensee's Standards and Practices. Placement of the commercial units is subject to Licensee's sole discretion, in each instance.

12. Promotion and Marketing Support. Licensor shall cooperate with Licensee on the marketing and promotion plan for Licensee and its Telecast of the Programs. In connection therewith, Licensor shall: [INCLUDE MARKETING OBLIGATIONS]

13. Publicity; Trademarks. Licensor grants to Licensee the right to issue and authorize advertising and publicity in connection with the Event, each Program, and the Network, including the names, photographs, likeness, acts, poses, voices and other sound effects of the participants, including the Event logos, the sponsors, and all other persons rendering services in connection with the Programs. On a non-exclusive basis, Licensor hereby licenses to Licensee, and Licensee has the right to use, the trademarks, service marks, logos, copyrights and related rights owned or controlled by Licensor

and/or the Event owners in connection with the advertising, marketing, and promotion of the Programs and the Network.

14. Representations and Warranties.
    a. Licensor represents and warrants that:
        i. Licensor has the right to enter into and perform this Agreement and grant the rights granted herein; has taken all necessary action to authorize the execution and delivery of this Agreement; and this Agreement does not and will not violate any provisions of any other agreement to which it is a party;
        ii. Licensor has sole and exclusive control of any and all media rights worldwide to the Event;
        iii. There are, and will be, no claims, liens, encumbrances or rights of any nature in or to the Licensed Footage or any part thereof which can or will impair or interfere with the rights, privileges or licenses of Licensee hereunder. "Licensed Footage" shall be defined as the Programs and each and every element thereof, including Licensor Ancillary Materials but specifically excluding Licensee Materials;
        iv. The use and exhibition of the Licensed Footage and each and every part thereof, including the sounds and music synchronized therewith, and the exercise of any right herein granted to Licensee, will not violate or infringe upon the trademark, trade name, copyright, patent, literary, dramatic, music, artistic, personal, private, contract, civil or property right, right of privacy or publicity, or any other right of any person or constitute a libel or slander of any person, and the Licensed Footage will not contain any unlawful or censorable material;
        v. Licensor has not and will not sell, assign, transfer, convey or hypothecate to any person or company, any right, title, or interest in or to the Licensed Footage, or any of the other rights granted to Licensee;
        vi. No lawsuits are, or shall be, threatened or pending in connection with the Licensed Footage;

    b. Licensee represents and warrants to Licensor as follows:
        i. Licensee has the right to enter into and perform this Agreement;
        ii. Licensee has taken all necessary action to authorize the execution and delivery of this Agreement; and
        iii. This Agreement does not and will not violate any other agreement to which Licensee is a party.

15. Indemnification. Licensor agrees to indemnify and hold Licensee (and Licensee's affiliates, exhibitors, assignees, licensees, and its respective directors, officers and employees) harmless against any liability, damage, costs and expenses (including reasonable attorneys' fees) arising out of any claim, demand or action in connection with the following: (i) a breach of any representation, grant, warranty or agreement assumed by Licensor hereunder; and (ii) personal injury to or death of a person or damage to property to the extent caused by the acts, errors and/or omissions, or the willful misconduct of Licensor or Licensor's officers, directors, agents, employees, subcontractors or volunteers. Licensee will give Licensor prompt notice of any claim to which the foregoing indemnity applies. Licensee may participate in the defense of the same, at its expense, through counsel of its choosing. The final control and disposition of the same remains with Licensor, but no such claims may be settled by Licensor in a manner prejudicial to Licensee's rights hereunder without the consent of the Licensee, not be unreasonably withheld. This section survives the termination or expiration of this Agreement.

16. Insurance. [INSERT INSURANCE REQUIREMENTS]

17. Compliance with Law; FCC Regulations. Licensor warrants and represents that the Programs comply with all applicable federal, state and local laws, rules and regulations, including, but not limited to,

the rules and regulations of the Federal Communications Commission ("FCC"). Specific reference is hereby made to Section 507 of the Communications Act of 1934, as amended (the "Communications Act") which makes it a criminal offense for any person to accept or pay, or agree to accept or pay, any money, services or other valuable consideration for the inclusion of any material or play as part of a television or radio program without disclosing the fact of such payment or agreement. Licensor acknowledges that it is familiar with the requirements of the Communications Act and agrees that it shall not accept, pay or agree to accept or pay any money or other valuable consideration for the inclusion of any material or plug as part of the Programs, without written notice to Licensee and without adequate disclosure as required by the Communications Act and the rules and regulations of the FCC. This section survives the termination of this Agreement.

18. Termination. Licensee has the right to terminate this Agreement in the event of any material breach by Licensor of any provision, agreement or obligation hereunder that is not cured, if capable of being cured, by Licensor within ten (10) business days of receiving notice of such breach.

19. Miscellaneous.
    a. Force Majeure. Notwithstanding anything herein contained to the contrary, neither party is liable to the other in damages because of any failure to perform hereunder caused by any cause beyond its control, including, but not limited to, natural disaster, accident, casualty, labor controversy, civil disturbance, embargo, war, threat of war, act or threat of terrorism, act of God, any government ordinance or law, the issuance of any executive or judicial order, or any failure or delay with respect to transmission equipment or apparatus.

    b. Relationship. Nothing contained herein is construed so as to constitute a partnership, agency or joint venture between the parties. Instead, the relationship between the parties is at all times that of independent contracting parties. As between each other, each party is fully responsible for all persons and entities it employees or retains, except as otherwise specifically provided in this Agreement.

    c. Notices. All notices and other communications required or permitted to be given under this Agreement must be in writing and deemed to have been duly given if: (i) delivered personally; (ii) mailed, via certified or registered mail with postage prepaid; or (iii) sent by next-day or overnight mail or delivery. All such notices will be deemed given on the date actually delivered (except if such date is a Saturday, Sunday or legal holiday, in which case it will be deemed given on the next business day). If a party delivers any notice to the other party in a manner that does not comply with this Subsection 19(c), then the same will be deemed delivered on the date, if any, on which the other party actually receives such notice. Each party's address for notices is as set forth in the preamble above or, in each case, at such other address as may be specified in writing to the other parties hereto.

    d. Confidentiality. Each party recognizes and acknowledges that it may receive certain confidential information and trade secrets concerning the business and affairs of the other party and/or its trustees, officers, executives, and affiliates which may be of great value to the disclosing party ("Confidential Information"). As such, the receiving party agrees not to disclose, unless either party is required by a court, tribunal or governmental or regulatory agency, or by law or legal order, any Confidential Information of the other party, or any of the terms or conditions of this Agreement (including this Agreement in its entirety or any documents delivered in accordance herewith), to any third-party other than the receiving party's legal and/or financial advisors who need to know such information in order to render services on behalf of the receiving party, or in any way use such information other than as reasonably necessary to perform this Agreement. If disclosing such information in response to a law or legal order, the receiving party shall give prior

written notice within a reasonable time to the disclosing party and make a reasonable effort to protect and/or limit such information from unnecessary disclosure or use. Notwithstanding the foregoing, Licensee may disclose the terms hereof to any parent or sister company who will be under the same confidentiality obligations as detailed herein. This Subsection 19(d) survives the termination of this Agreement.

e. Severability; Waiver. Nothing contained herein is construed to require the commission of any act contrary to law, and wherever there is any conflict between any provisions contained herein and any present or future statute, law, ordinance, or regulation contrary to which the parties have no legal right to contract, the latter prevails; but, the provision of this Agreement which is affected is curtailed and limited only to the extent necessary to bring it within the requirements of the law. Failure of any party at any time to require performance of any provision of this Agreement does not limit the party's right to enforce the provision, nor does any waiver of any breach of any provision be a waiver of any succeeding breach of the provision or a waiver of the provision itself or any other provision.

f. Construction. The laws of [INSERT STATE] govern all matters arising under or relating to this Agreement, without regard to its conflict of law principles. The parties agree that any legal action brought with respect to this Agreement must be brought in the state or federal courts in [INSERT JURISDICTION] and hereby submit to the jurisdiction of such courts.

g. Assignment. Licensor shall not assign any right nor delegate any obligation under this Agreement. Any attempted assignment or delegation by Licensor is null and void. Licensee may assign any right or delegate any obligation under this Agreement to any corporate successor or any entity controlled by, under common control with or controlling Licensee. This Agreement binds and benefits the parties and their respective permitted successors and assigns.

h. Entire Agreement. This Agreement is the final and exclusive agreement between the parties on the matters contained in this Agreement. All previous and contemporaneous negotiations, representations and agreements, whether written or oral, between the parties concerning the subject matter of this Agreement are merged into this Agreement. The parties may amend this Agreement solely by written agreement, signed by both parties.

This Agreement is hereby executed by a duly authorized representative of each party as of the Effective Date.

Entertainment and New Media

2019 NYSBA Annual Meeting, IP Section

New York Hilton Midtown

January 15, 2019

Frankfurt Kurnit Klein + Selz PC

Introductions

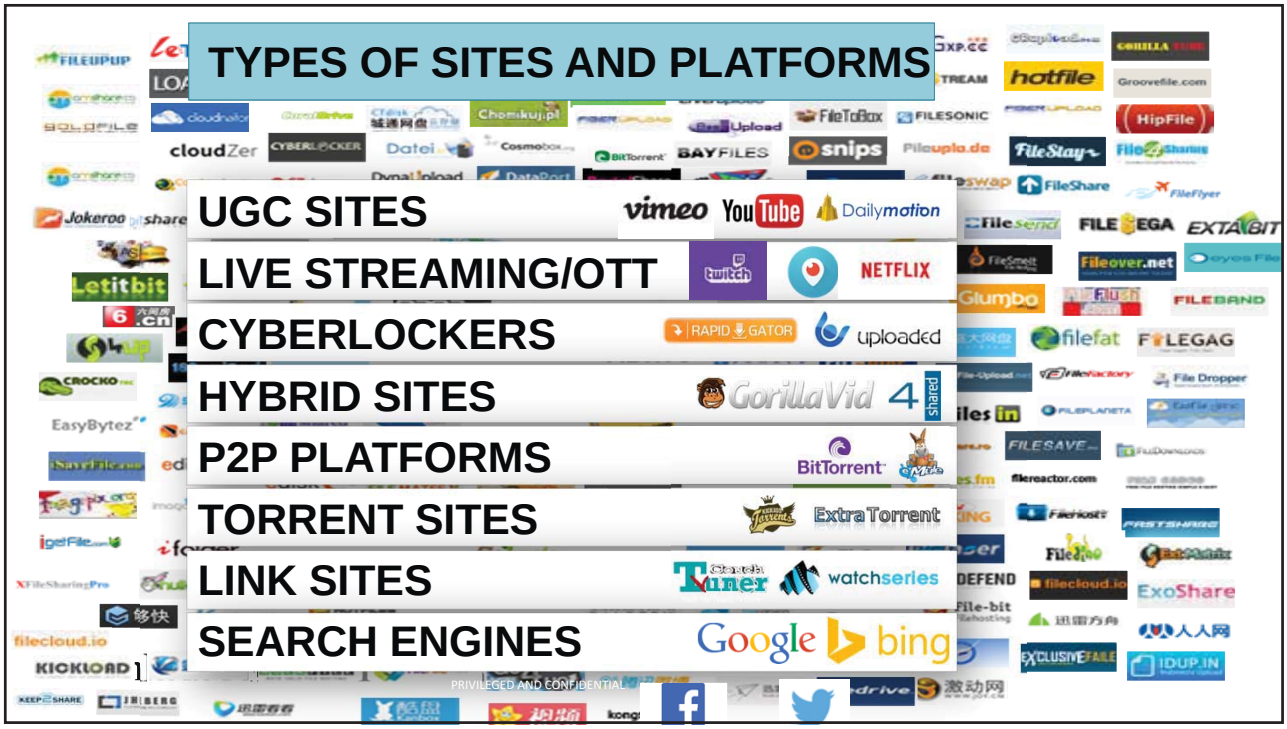
- Jemar Daniel, Esq.: Viacom
- Catherine Farrelly, Esq.: Frankfurt Kurnit
- Deborah Robinson, Esq.: Viacom
- Adrian D. Stubbs, Esq.: CBS Television
- Matthew Winterroth, Esq.: WWE

New Media and Enforcement Issues

Deborah Robinson, Esq.

VP & Senior Counsel, Anti-Piracy, Viacom

Frankfurt Kurnit Klein + Selz PC

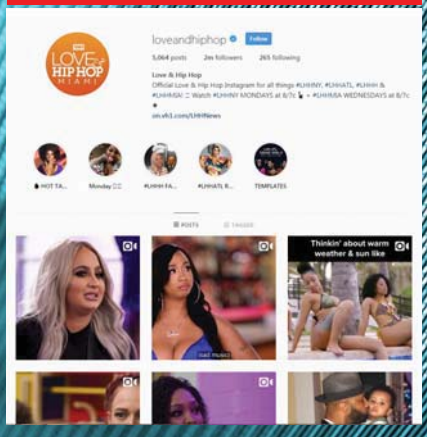


Types of Infringements

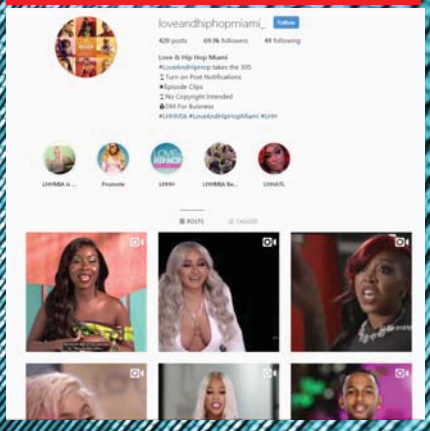
- LINEAR/TV CONTENT
- ONLINE CONTENT
- CONSUMER PRODUCTS
- APPS & GAMES
- SOCIAL MEDIA
- TICKETS & EVENTS

FAKE SOCIAL MEDIA ACCOUNTS

OFFICIAL INSTAGRAM PAGE



INFRINGING INSTAGRAM PAGE

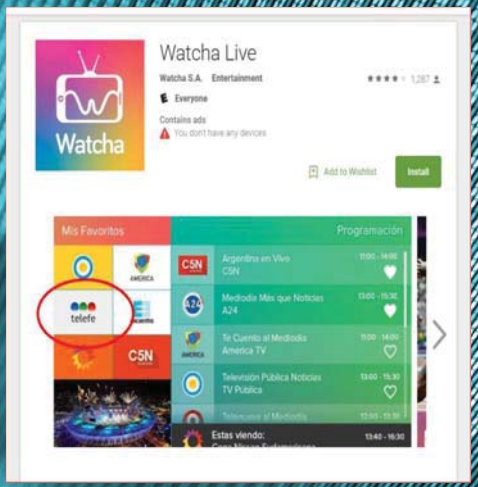


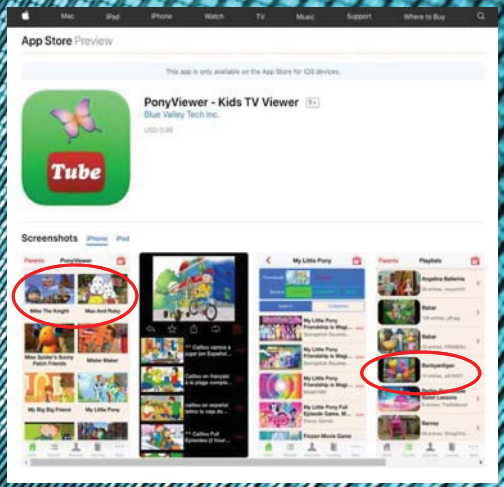
INFRINGING VIDEO?

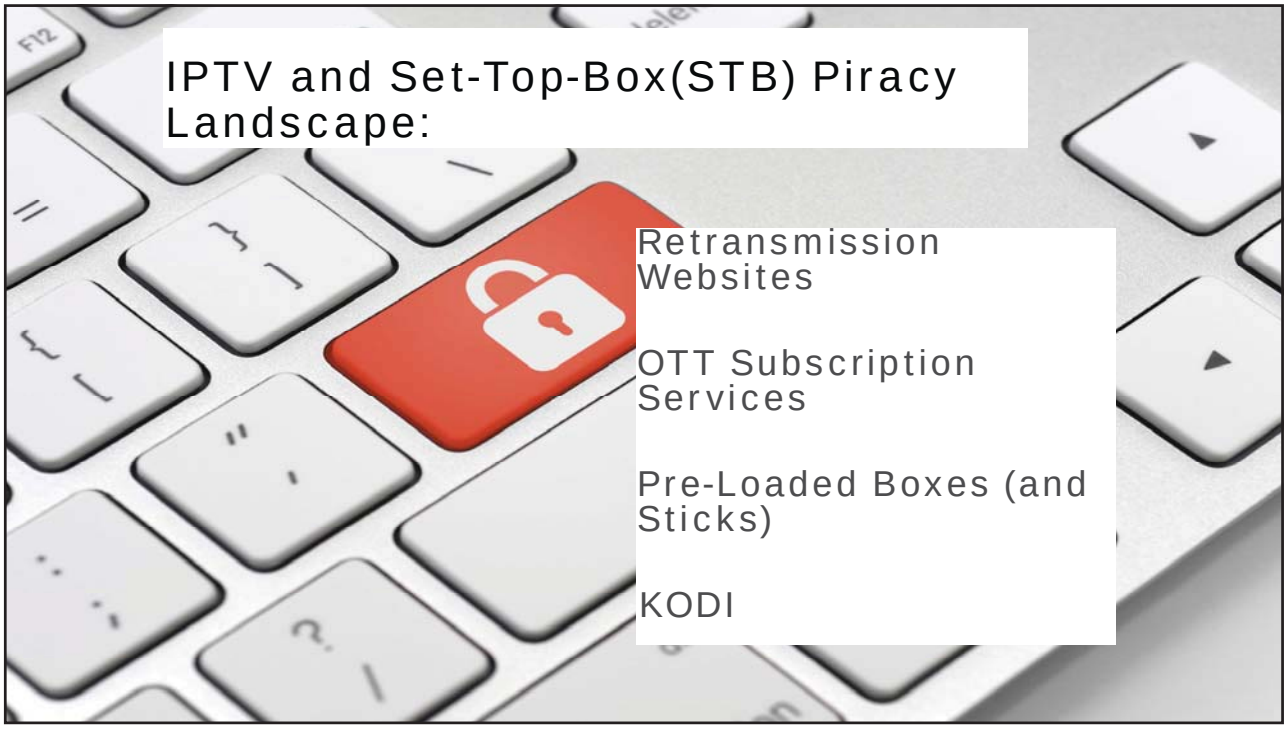
PAW PATROL VIDEO

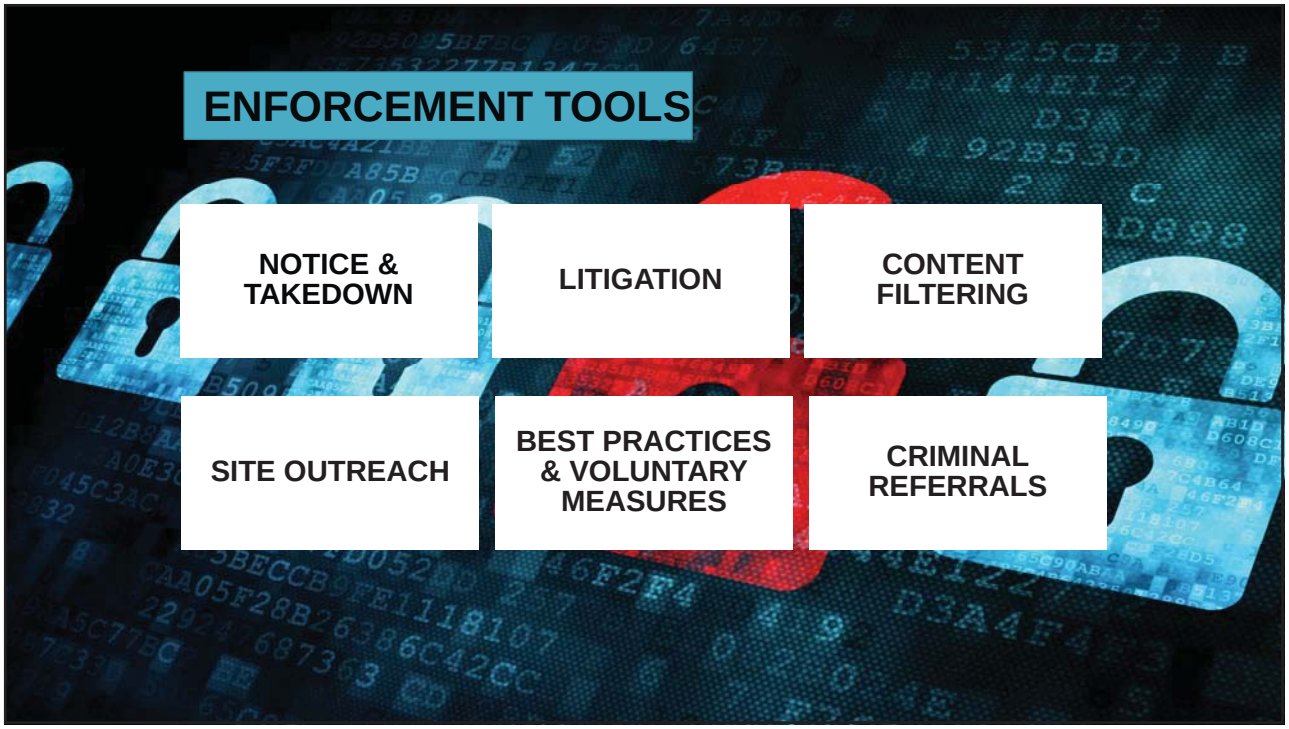
PAW PATROL GAME PLAY

INFRINGING MOBILE APPS






IPTV and Set-Top-Box(STB) Piracy Landscape:
Retransmission Websites
OTT Subscription Services
Pre-Loaded Boxes (and Sticks)
KODI


ENFORCEMENT TOOLS
NOTICE & TAKEDOWN
LITIGATION
CONTENT FILTERING
SITE OUTREACH
BEST PRACTICES & VOLUNTARY MEASURES
CRIMINAL REFERRALS

IP Enforcement Cheat Sheet

Matthew Winterroth, Esq.
VP, Intellectual Property
World Wrestling Entertainment, Inc.

Frankfurt Kurnit Klein+Selz PC

DMCA: Quick Recap

- The Digital Millennium Copyright Act (DMCA), 17 U.S.C. §§ 512, was created primarily as a solution for online service providers (OSPs) such as YouTube, Facebook, Twitter and Dailymotion that host content uploaded by third parties rather than solely create their own original content.
- OSPs benefit from the DMCA because it provides "safe harbor" from liability in the event content uploaded to their site infringes another's copyrights, so long as they adhere to certain provisions, including:

Frankfurt Kurnit Klein+Selz PC

DMCA: “Safe Harbor” Provisions

- Submit an OSP agent designation with the Copyright Office -- 17 U.S. Code § 512(c)(2)
  - The database is useful for determining the appropriate party to contact in the event a takedown notice needs to be filed.
  - https://www.copyright.gov/dmca-directory/

Frankfurt Kurnit Klein + Selz PC

DMCA: “Safe Harbor” Provisions

- Establish notice and takedown procedures -- 17 U.S. Code §§ 512(c)(1)(C), 512(c)(3)
  - Copyright owners may submit a list of allegedly infringing content to an OSP’s designated agent. Once an OSP has been made aware of infringing content, the content must be “expeditiously” removed, and the uploader be notified of the takedown.
  - The uploader can then file a counter-notification to contest the filing of a notice and takedown after content has been removed -- 17 U.S. Code §§ 512(g)(3). Doing so requires the uploader to give their true contact details and consent to jurisdiction of Federal District Court.
  - The content would then be restored, and the only way for the copyright owner to force content removal would be to file a lawsuit.

Frankfurt Kurnit Klein + Selz PC

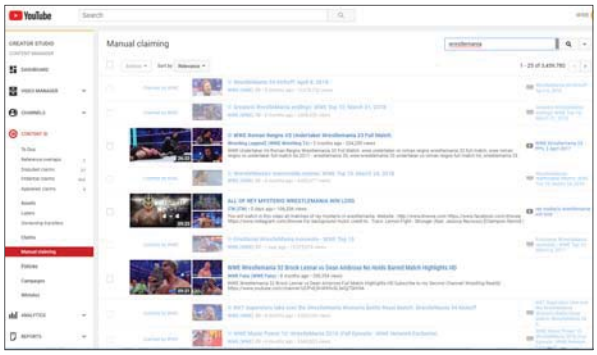
Evolution of Notice and Takedown

- As a result of the popularity of User Generated Content (UGC) and the progression of video, many OSPs evolved and have created forms for mass © takedowns and other IP rights.
- Others have more formal business relationships with copyright owners and formed more robust rights managers, allowing for asset fingerprinting and automated monetization and blocking of content.

Frankfurt Kurnit Klein + Selz PC

YouTube CMS and Content ID – Gold Standard

- As the copyright owner, you provide YouTube with a reference copy of your eligible content. YouTube uses the reference to scan uploaded videos for matching content, UGC and streaming. When a match is found, YouTube applies your preferred policy: to monetize, track, or block the video in question. Reporting/analytics is available.
- https://support.google.com/youtube/answer/3244015?hl=en
- https://www.youtube.com/watch?v=9g2U12SsRns



Frankfurt Kurnit Klein + Selz PC

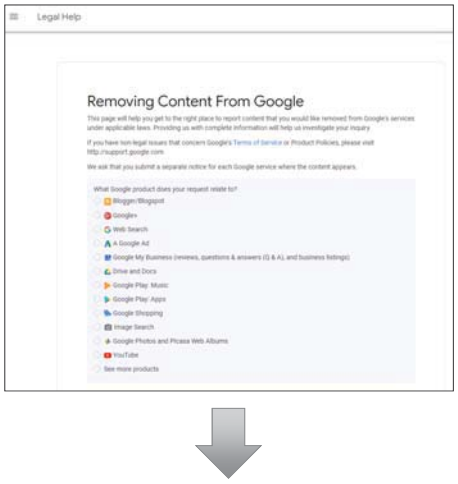
Other Ways to Enforce on YouTube

- Content Verification Program (CVP): https://support.google.com/youtube/answer/6005923
  - designed especially for copyright owners to issue multiple removal requests.
- Send a one-off DMCA takedown notice for content on YouTube: https://support.google.com/youtube/answer/2807622?hl=en&ref_topic=2778544
- Takedowns concerning other IP/legal violations (e.g. TM, counterfeit, privacy) : https://www.youtube.com/reportingtool/legal

Frankfurt Kurnit Klein+Selz PC

Other Google sites

- Each sub-site under the Google umbrella (e.g. Blogger, Search, Google Play, etc.) has a different method and form to request content removal
- https://support.google.com/legal/troubleshooter/1114905?hl=en

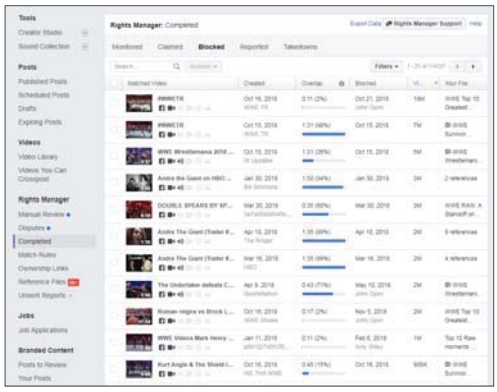


In response to a complaint we received under the US Digital Millennium Copyright Act, we have removed 2 result(s) from this page. If you wish, you may read the DMCA complaint that caused the removal(s) at LumenDatabase.org.

Frankfurt Kurnit Klein+Selz PC

Facebook/Instagram Rights Manager

- Similar to YouTube's CMS, Rights Manager is for content creators wanting to upload reference content and protect their works on Facebook or Instagram at scale.
- Newer and less robust than YouTube CMS. Monitors and enforces on UGC and streaming content. Reporting/analytics is available.
- https://rightsmanager.fb.com



Frankfurt Kurnit Klein + Selz PC

Other Ways to Enforce on FB/IG

- Facebook IP reporting portal:
  ©: https://www.facebook.com/help/contact/1758255661104383
  TM: https://www.facebook.com/help/contact/1057530390957243
  Counterfeit: https://www.facebook.com/help/contact/628238764025713
- Facebook takedowns concerning other legal violations and community standards violations:
  https://www.facebook.com/help/181495968648557?ref=community_standards
- Instagram infringement reporting portal:
  https://help.instagram.com/535503073130320

Frankfurt Kurnit Klein + Selz PC

Twitter/Periscope

- Twitter/Periscope currently does not have a content ID or rights manager program for content creators. Below are reactive tools to remove infringing content, but vs. other OSPs, Twitter is quite slow to react and requires more back and forth.

- Twitter/Periscope IP reporting portal:

  ©: https://help.twitter.com/forms/dmca

  TM: https://help.twitter.com/forms/trademark

  Counterfeit: https://help.twitter.com/forms/counterfeit

- Twitter takedowns concerning other legal violations and community standards violations: https://help.twitter.com/en/rules-and-policies/twitter-report-violation

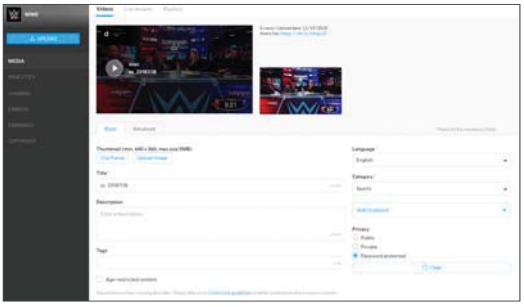
Frankfurt Kurnit Klein + Selz PC

DailyMotion

- DailyMotion is a video sharing platform, based in France, and owned by Vivendi. DailyMotion has a content management system, but it is not nearly as robust as YouTube's or even Facebook's: https://faq.dailymotion.com/hc/en-us/articles/203921173

- Copyright reporting portal: https://faq.dailymotion.com/hc/en-us/requests/new?ticket_form_id=136048&request%5Bcustom_fields%5D%5B30150188%5D=copyrightform-notification

- DailyMotion policies concerning other legal violations and community standards violations: https://faq.dailymotion.com/hc/en-us/categories/200290417-Copyright-Content-Policies



Frankfurt Kurnit Klein + Selz PC

Other Popular OSP Enforcement Tools

- **Twitch:**
  ©: https://www.twitch.tv/p/legal/dmca-guidelines; e-mail to dmca@twitch.tv
  TM: https://www.twitch.tv/p/legal/trademark-policy; e-mail to trademarkclaims@twitch.tv

- **Vimeo:**
  ©: https://vimeo.com/dmca/claim or e-mail to dmca@vimeo.com
  TM: https://vimeo.com/help/violations/trademark
  Privacy: https://vimeo.com/help/violations/privacy

- **Snapchat:**
  ©: https://support.snapchat.com/en-US/co/report-copyright
  TM/counterfeit: https://support.snapchat.com/en-US/a/infringement-trademark-general
  Right of Publicity: https://support.snapchat.com/en-US/a/infringement-publicity

Frankfurt Kurnit Klein + Selz PC

Growing and Protecting Your Brand

Adrian D. Stubbs, Esq.
Assistant General Counsel, CBS Television

Frankfurt Kurnit Klein + Selz PC

Trademark Clearance

Catherine M.C. Farrelly, Esq.

Partner, Frankfurt Kurnit Klein + Selz

Frankfurt Kurnit Klein + Selz PC

Trademark Clearance and Filing

- **Clearance Searches** – Search in each territory or accept business risk of conflict.
- **Filing Considerations** – International nature of esports and other businesses conducted online, particularly where they have international viewership and related merchandise.
- **What To File** – Depending on the country and your business plans, file either an application in each country or a multi-national filing, in territories such as Europe, where that is available under an international treaty.
- **Where To File** – Prioritize regions or countries, or search and file in waves. Consider trademark squatting issues.

Frankfurt Kurnit Klein + Selz PC

Platform Specific Content Review Considerations

Jemar Daniel, Esq.

VP & Senior Counsel, Business Legal Affairs, Viacom

Frankfurt Kurnit Klein + Selz PC

Linear Content Review Considerations

Each platform presents unique considerations that can elevate or mitigate the risks of receiving a claim on the content distributed

Considerations for linear programming that elevate risks:

- Difficult to remove show from programming schedule on request (court ordered or based on settlement agreement)
  - Negatively impacts the Ad-Sales team who sells commercial space adjacent to the removed program
- For now- still the dominant means of content consumption which means more visibility and possible legal exposure

Considerations for linear programming that mitigate risks:

- Longer content review window
- Structured production process and well developed information exchange between Production, Legal, and other network stakeholders
- Trained personnel in production management and creative groups
- Solvent 3rd party prodco partners to indemnify network in legal matters

Frankfurt Kurnit Klein + Selz PC

Digital Content Review Considerations

Considerations for digital programming that elevate risks:

- Shorter content review window
- More programming volume given the low production cost
- Generally project based production staff and high turnover from project to project
- Generally less experienced (sometimes less solvent) 3rd party prodco partners
- Generally heavier reliance of "fair-use" on content created specifically for digital consumption
- Heavy incorporation of 3rd party assets or marks (e.g., Instagram, FB, YouTube, Snap, etc.) in show content
- Lower budgets to pay out jury awards or settlements

Considerations for digital programming that mitigate risks:

- Easier to take down if not subject to advertiser commitment
- Slightly lower visibility (not as popular as linear (yet))
- Content produced specifically for digital consumption can get lost in the sea of other content available digitally

Frankfurt Kurnit Klein + Selz PC

Social Media Influencers and Endorsements

Catherine M.C. Farrelly, Esq.

Partner, Frankfurt Kurnit Klein + Selz

Frankfurt Kurnit Klein + Selz PC

Frankfurt Kurnit Klein + Selz PC

Frankfurt Kurnit Klein + Selz PC

Questions?

Frankfurt Kurnit Klein & Selz PC
488 Madison Avenue
New York, NY 10022
(212) 826 5577
dmaggiacomo@fkks.com
cfarrelly@fkks.com

Frankfurt Kurnit Klein + Selz PC

Advertising, Social Media and the FTC

Barry Benjamin, Esq.
Kilpatrick Townsend LLP

Nur-ul Haq, Esq.
VP & Counsel, Tech & Kids Compliance, Viacom

Ann Gorfinkle, Esq.
VP, Standards and Practices for Nickelodeon, Viacom

Rebecca Leigh Griffith Esq.
Senior Counsel, Unilever United States, Inc.

ADVERTISING, SOCIAL MEDIA, & THE FTC

New York State Bar Association
Annual Meeting 2019

Intellectual Property Law Section

January 15, 2019

Barry M. Benjamin
Kilpatrick Townsend

Nur-ul Haq, Esq.
Viacom

Anne Gorfinkel
Viacom

Rebecca Leigh Griffith, Esq.
Unilever United States, Inc.

With the expansion of social media and the introduction of new digital platforms, brands are looking to connect with consumers in fast, real-time, personalized ways. Brands have gravitated towards and embraced the opportunity to participate in influencer marketing through these different social media. With influencer marketing, brands can connect with consumers by engaging a specific individual to post and share information about a product or service. These posters, who are known as "influencers," generally have a large or specific audience that brands want to target. This multimillion dollar business has boomed in recent years with new platforms and opportunities to connect with consumers.

Influencer marketing can take place in a variety of situations; for example, an influencer may post: (1) a YouTube video, reviewing make-up products; (2) on Facebook, touting a new restaurant; (3) a fashion blog entry, noting new clothing brands; (4) a video on Snapchat, which includes a discount code for purchasing workout equipment; or (5) on Instagram, highlighting a unique travel destination. The common thread with each of these different types of marketing avenues is the ability to connect on a personalized level with the consumer and provide targeted advertising for a specific product or service.

However, these mediums and opportunities for using influencer marketing have opened the doors for emerging legal issues and considerations. Specifically, brands must be aware of, and analyze the implications of, advertising laws, and incorporate disclosures into the posts to alert consumers of the relationship between the influencer and the advertiser.

A. Legal Framework

Influencer marketing is guided by general advertising laws. Specifically, 15 U.S. Code § 45 provides that "unfair or deceptive acts or practices in or affecting commerce . . . are . . .

declared unlawful."[i] This regulation has broad and wide implications and applies to the use of influencer marketing and sponsored advertising. Brands have the responsibility to ensure that influencers who have a material connection to the brand, either in terms of compensation, employment, free goods or services or other consideration, explicitly disclose the connection. A disclosure ensures that consumers are not misguided, or deceived, by the reasons or motivations behind a post, comment or endorsement.

The FTC has also provided its guidance in the Guides Concerning Use of Endorsements and Testimonials in Advertising (the "Guidelines").[ii] The Guidelines, as explained by the FTC, "reflect the basic truth-in-advertising principle that endorsements must be honest and not misleading. An endorsement must reflect the honest opinion of the endorser and can't be used to make a claim that the product's marketer couldn't legally make."[iii] The Guidelines are intended to assist advertisers, consumers, and influencers in understanding the basic principles, best practices and required disclosures for an influencer who is posting about a product or service for which he or she has received compensation.

The Guidelines explain that disclosures must be included in any type of post, no matter the medium or platform, where there is a relationship with the advertiser. If there is the implication that the influencer is sponsoring, or endorsing a product or service, and there is a material connection with the advertiser, there must be a disclosure within the post.[iv]

The question then becomes what constitutes an adequate disclosure? It is understood that the disclosure will vary depending on the medium on which it is posted, but the underlying requirement is that the disclosure must "provide the essential information"[v] and must be "worded in a way that's understandable to the ordinary reader."[vi] The best disclosure fully explains the relationship between the influencer and advertiser, and is clear, prominent, and conspicuous. For

example, if an influencer is given a free product, the optimal disclosure would state "Company X gave me this product to try . . . ."[vii] The disclosure can be included directly in the text of a post or explicitly stated within a video.

The FTC has also provided recommendations for what it means to "make a disclosure clear and conspicuous." This includes making the disclosures "close to the claims to which they relate; in a font that is easy to read; in a shade that stands out against the background; for video ads, on the screen long enough to be noticed, read, and understood; and for audio disclosures, read at a cadence that is easy for consumers to follow and in words consumers will understand."[viii] These general rules can be applied for every type of post and on every social media platform.

In addition, specific guidelines apply to the different social media platforms because consumers see and read the sponsored posts in different ways. On Instagram, it is important that the disclosure is included within the first three lines of text; if there is additional text, the remaining text will be truncated and consumers will need to click "more" to read the entire post, something they may not do.[ix] For Instagram and Snapchat stories, the disclosure should be superimposed over the video and be "easy to notice and read in the time that [] followers have to look at the image."[x] On Twitter, where the length of the post is limited by the number of characters, simple words can be included as disclosures. For example, one can use "#sponsored," "#promotion," "#paid ad," or "#ad."[xi] Again, the point is that the disclosure be clear and conspicuous and that "people get the information they need to evaluate sponsored statements."[xii]

B. Instructive Cases and Orders

Most of the legal guidance regarding influencer marketing has come from the FTC, either in the Guidelines or through FTC complaints and notices to influencers and advertisers. A few of the more instructive cases are below.

- ***CSGOLotto, Trevor Martin, and Thomas Cassell.***[xiii] In the FTC's first enforcement action against social media influencers, the FTC filed a complaint against Trevor "TmarTn" Martin and Thomas "Syndicate" Cassell, who posted endorsements of the gambling website CSGOLotto, without disclosing that they were the owners of the site.[xiv] In addition, the influencers allegedly paid other well-known influencers to post about the website, without requesting that the influencers include disclosures in their posts. The action was eventually settled, requiring that Martin, Cassell, and the CSGOLotto company "clearly and conspicuously disclose any material connections with an endorser or between an endorser and any promoted product or service."[xv]
- ***Cole Haan.***[xvi] Here, the FTC took issue with Cole Haan's "Wandering Sole" contest on Pinterest, which asked participants to create Pinterest boards with images of five Cole Haan shoes and photographs of the contestants' "favorite places to wander."[xvii] The person who posted the most creative entry would win a $1,000 shopping spree. Cole Haan told participants to include the hashtag "#WanderingSole" with their photos, but Cole Haan did not tell or require participants to make it clear that they posted the pins in order to enter a contest. The fact that this material connection (that a pin resulted in a contest entry) was not disclosed in entrants' posts concerned the FTC. Although the FTC ultimately did not bring an enforcement action, the FTC stated, in its closing letter, that "entry into a contest to receive a significant prize in

exchange for endorsing a product through social media constitutes a material connection that would not reasonably be expected by viewers of the endorsement." In the FTC's view, the #WanderingSole hashtag did not effectively communicate the material connection between Cole Haan and the contest participants.

- ***Lord & Taylor, LLC.***[xviii] Lord & Taylor partnered with online fashion magazine Nylon to engage Instagram influencers for a marketing campaign to promote a specific paisley dress.[xix] Lord & Taylor gave the dress to fifty influencers and paid them to post photos of themselves in the dress on Instagram during a particular weekend in March 2015, and Nylon ran an article and posted a photo to its own Instagram account promoting the dress. Although Lord & Taylor pre-approved the posts, Lord & Taylor did not require, among other things, that the influencers disclose that they were paid to post the photos or had received the dress for free. The FTC complaint charged Lord & Taylor with three violations: (1) that Lord & Taylor falsely represented that the Instagram posts reflected the independent statements of impartial fashion influencers; (2) that Lord & Taylor failed to disclose that the influencers were the company's paid endorsers; and (3) that Lord & Taylor falsely represented that the Nylon article and Instagram post reflected Nylon's independent opinion about the dress. The case settled with requirements for stricter oversight and a more robust mechanism for monitoring campaigns and necessary disclosures.[xx]
- ***Warner Bros. Home Entertainment Inc.***[xxi] Warner Bros. conducted a marketing campaign for the video game *Middle Earth: Shadow of Mordor*.[xxii] Warner Bros hired an influencer marketing agency to execute a YouTube campaign with top gaming influencers. A select group of YouTubers were given a pre-release version of the

video game and were each paid anywhere from a few hundred to tens of thousands of dollars to promote the game on their channels. The influencers were instructed to create and post gameplay videos that promoted the game in a positive way and not to disclose any bugs or glitches they encountered. In addition, the influencers were told to disclose the sponsorship in the description box below the video, which often resulted in the disclosure being "below the fold" and visible only if consumers clicked on a "show more" link. A year after the campaign had ended, the FTC filed a complaint against Warner Bros. The FTC took the position that the marketing campaign misled consumers by suggesting that the videos reflected the independent or objective views of the influencers and that the disclosures were inadequate. The Guidelines clearly state that the disclosure must be near the top of the description box, above the "Show More" button, and for videos, the Guidelines require that influencers also include a verbal disclosure close to the beginning of the video. Under the FTC's order, Warner Bros. is "barred from failing to make such disclosures in the future and cannot misrepresent that sponsored content, including gameplay videos, are the objective, independent opinions of video game enthusiasts or influencers."[xxiii]

- ***FTC Warning Letters*.** In April 2017, the FTC sent out more than 90 letters to remind "influencers and marketers that influencers should clearly and conspicuously disclose their relationships to brands when promoting or endorsing products through social media."[xxiv] The letters were the result of petitions filed by Public Citizen and affiliated organizations; this was the first time that the FTC contacted influencers directly to warn them about the way in which the influencers either improperly, or failed completely, to disclose their relationships with advertisers. In addition to

explaining the purpose for including disclosures, and the best practices for doing so, the letters specifically addressed three trends within disclosures. The FTC noted that "when multiple tags, hashtags, or links are used, readers may just skip over them," and therefore the disclosures are not considered conspicuous. The FTC also noted that shortened, or abbreviated, disclosures are not necessarily clear. For example, "#sp," "Thanks [Brand]," or "#partner" do not necessarily describe that the post is sponsored.[xxv] And, the FTC reminded influencers that consumers must be able to see the disclosure clearly without having to search for it within the post.

After the initial warning letters were sent, the FTC wrote follow-up letters to some of these influencers in September 2017.[xxvi] These letters cited specific posts that the FTC determined were not in compliance with the Guidelines. Instead of just being a general "warning letter," these follow-up letters asked the influencers to inform the FTC as to whether there was a "material connection to the brands in the identified social media posts." The FTC also requested that if the influencers do have a connection, that they specifically detail the steps that they will take to ensure that "they clearly disclose their material connections to brands and businesses."

C. Practical Considerations and Best Practices

Brands must be sensitive to the need for adequate disclosures in all sponsored advertisements. Of course, the most important rule is to ensure that the relationship between the influencer and the brand is fully, clearly, and prominently disclosed, but there are additional important considerations.

First, many social media platforms are creating new tools for directly indicating that a post is sponsored by a brand. It is important not to rely on these tools to inform consumers about the relationship for a few reasons. First, if a consumer is unaware, or not knowledgeable about a specific social media tool, the consumer may not understand that the post is sponsored. Additionally, the tool may ultimately be removed from the platform, leaving the post without any type of disclosure. If the disclosure is included directly within the text or video, then both the brand and the influencer will be confident that the disclosure will last the entire life of the post. Lastly, these tools may not provide the influencer with the opportunity to include a full disclosure or provide a way to accurately describe the relationship behind the post.

Many brands want to create custom hashtags for their marketing campaign, and will try to incorporate the words “ad” or “sponsored” to comply with the disclosure requirements. However, these hashtags may be too lengthy or confusing, making it difficult for the average consumer to understand that the hashtag is a marketing disclosure. If a brand wants to include a custom hashtag, it is recommended that the influencer also include a simple tag such as “ad” or “sponsored” so that a clear and conspicuous disclosure is included within the post.

Brands should always keep the Guidelines in mind when new social media platforms emerge. The new platforms may provide different ways for sharing content, which may not always provide the traditional text options. Accordingly, it is important for both the brands and the influencers to be creative and ensure that the post explains the relationship and that the post is sponsored.

When engaging an influencer to post about a certain product or service, a brand should take the initiative to provide the influencer with the necessary tools to properly comply with the Guidelines. This includes informing the influencer about his or her responsibility for disclosing

the relationship. If a product is shared with an influencer for free, and there is no contractual relationship to post about the item, then the brand should include a note explaining that if the influencer decides to post about the product, then he or she must explain that the item was given to the influencer for free. In the alternative, if there is a contractual relationship between the influencer and the brand, then the brand may want to include specific requirements regarding the posts. This could include, the specific language to include, the specific hashtags to use, the language not to use, or even exactly what the picture or video should look like.

It is also important for the brand owners to pre-approve posts, if feasible, and monitor the posts once they are published. A brand owner's responsibility to ensure that the posts comply with the Guidelines does not end when the instructions are provided. Instead, the brand owner must continue to confirm that the disclosures are accurately included, and if they are not, provide the influencer with instructions on how to correct the post.

In sum, the following are a few best practices to help minimize the legal risks when engaging influencers in advertising:

- Contractually require influencers to abide by the Guidelines and provide clear instructions on how and when to disclose. Consider providing the actual disclosure language to the influencer.
- Monitor influencers' posts and ensure that disclosures are present and sufficient.
- Do not use ambiguous disclosures such as #ambassador, #partner, #sp, #spon, or #thanks. The FTC has stated that disclosures should use clear and unmistakable language.
- Make sure that disclosures accompany the post in a prominent location and do not bury the disclosures in links or text below a video or image.
- Do not simply reply on a platform's own disclosure tool. The disclosure obligation rests with the brand, and the brand should make sure that its disclosures are sufficient and lasting.

- Do not assume that a relationship is obvious. While it may seem that everyone would know that a celebrity has a business relationship with a product, the best practice is to err on the side of caution and disclose.

If participants enter a contest or sweepstakes with social media posts, the FTC will likely view this as a material connection and a disclosure must accompany the post.

THIS OUTLINE PROVIDES GENERAL GUIDELINES ONLY AND SHALL NOT BE CONSIDERED LEGAL ADVICE.

---

[i] 15 U.S.C. § 45(a)(1).

[ii] FED. TRADE COMM'N, THE FTC ENFORCEMENT GUIDES: WHAT PEOPLE ARE ASKING, *available at* https://www.ftc.gov/tips-advice/business-center/guidance/ftcs-endorsement-guides-what-people-are-asking.

[iii] *Id.*

[iv] *Id.*

[v] *Id.*

[vi] *Id.*

[vii] *Id.*

[viii] *Id.*

[ix] *Id.*

[x] *Id.*

[xi] *Id.*

[xii] *Id.*

[xiii] *CSGOLotto, Trevor Martin, and Thomas Cassell*, No. C-4576 (Nov. 28, 2017), *available at* https://www.ftc.gov/enforcement/cases-proceedings/162-3184/csgolotto-trevor-martin-thomas-cassell.

[xiv] Press Release, Fed. Trade Comm'n, CSGO Lotto Owners Settle FTC's First-Ever Complaint Against Individual Social Media Influencers (Sept. 7, 2017), *available at* https://www.ftc.gov/news-events/press-releases/2017/09/csgo-lotto-owners-settle-ftcs-first-ever-complaint-against.

[xv] *Id.*

[xvi] *Cole Haan*, No. 142-3041 (F.T.C. Mar. 20, 2014).

[xvii] Fed. Trade Comm'n, Div. of Advert. Practices, Letter from Assoc. Dir. Mary K. Engle to Christie Grymes Thompson (March 30, 2014), *available at* https://www.ftc.gov/system/files/documents/closing_letters/cole-haan-inc./140320colehaanclosingletter.pdf.

[xviii] *Lord & Taylor, LLC*, No. C-4576 (F.T.C. May 23, 2016), *available at* https://www.ftc.gov/system/files/documents/cases/160523lordtaylordo.pdf.

[xix] Press Release, Fed. Trade Comm'n, Lord & Taylor Settles FTC Charges It Deceived Consumers Through Paid Article in an Online Fashion Magazine and Paid Instagram Posts by 50 "Fashion Influencers", *available at*

https://www.ftc.gov/news-events/press-releases/2016/03/lord-taylor-settles-ftc-charges-it-deceived-consumers-through.

[xx] Press Release, Fed. Trade Comm'n, FTC Approves Final Lord & Taylor Order Prohibiting Deceptive Advertising Techniques, *available at* https://www.ftc.gov/news-events/press-releases/2016/05/ftc-approves-final-lord-taylor-order-prohibiting-deceptive.

[xxi] *Warner Bros. Home Entertainment Inc.*, No. C-4595 (F.T.C. Nov. 17, 2016), *available at* https://www.ftc.gov/enforcement/cases-proceedings/152-3034/warner-bros-home-entertainment-inc-matter.

[xxii] Press Release, Fed. Trade Comm'n, Warner Bros. Settles FTC Charges It Failed to Adequately Disclose It Paid Online Influencers to Post Gameplay Videos, *available at* https://www.ftc.gov/news-events/press-releases/2016/07/warner-bros-settles-ftc-charges-it-failed-adequately-disclose-it.

[xxiii] Press Release, Fed. Trade Comm'n, FTC Approves Final Order Requiring Warner Bros. to Disclose Payments to Online Influencers, *available at* https://www.ftc.gov/news-events/press-releases/2016/11/ftc-approves-final-order-requiring-warner-bros-disclose-payments.

[xxiv] Press Release, Fed. Trade Comm'n, FTC Staff Reminds Influencers and Brands to Clearly Disclose Relationship, *available at* https://www.ftc.gov/news-events/press-releases/2017/04/ftc-staff-reminds-influencers-brands-clearly-disclose.

[xxv] *Id.*

[xxvi] Fed. Trade Comm'n, Div. of Advert. Practices, Letter from Assoc. Dir. Mary K. Engle (Sept. 6, 2017), *available at* https://www.ftc.gov/system/files/attachments/press-releases/los-propietarios-de-csgo-lotto-resuelven-la-primera-demanda-jamas-entablada-contra-influyentes-de/instagram_influencer_warning_letter_template_9-6-17.pdf.

[xxvii] Lesley Fair, FED. TRADE COMM'N, *Business Blog*, (Sept. 7, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/09/three-ftc-actions-interest-influencers.

NYS Bar Intellectual Property Law Section

Advertising, Social Media, & the FTC

2019 Annual Meeting CLE Program

January 15, 2019

KILPATRICK TOWNSEND

Panel Participants

- **Barry M. Benjamin, Esq.,** Kilpatrick Townsend LLP
  Partner
- **Nur-ul Haq, Esq.,** Viacom
  VP & Counsel, Tech & Kids Compliance
- **Anne Gorfinkle,** Viacom
  VP, Standards and Practices for Nickelodeon
- **Rebecca Leigh Griffith, Esq.,** Unilever US
  Senior Counsel

2

KILPATRICK TOWNSEND

Background

FTC has long kept a hard line between advertising and editorial.

NEWS RELEASE

FEDERAL TRADE COMMISSION

Washington, D.C. 20580

OFFICE OF INFORMATION 393-6800 Ext. 197

For RELEASE: IMMEDIATE, Tuesday, November 28, 1967

Statement in Regard to Advertisements That Appear in Feature Article Format

The Commission has recently considered the publication by various print media of advertisements that use the format and have the appearance of news or feature articles. Generally the caption "ADV." or "ADVERTISEMENT" appears at the top of such advertisements, but sometimes it is omitted. The Commission is concerned that omission of the caption "ADVERTISEMENT" may cause readers to believe that the advertisement is in fact a feature or news article. The Commission also wishes to point out that in some instances the format of the advertisement may so exactly duplicate a news or feature article as to render the caption "ADVERTISEMENT" meaningless and incapable of curing the deception.

3

KILPATRICK TOWNSEND

"Advertorials"

- **Adver**tisements designed to look like edi**torials**.
- In the 1980s and 1990s, FTC began regulating advertorials as potentially misleading (See 1983 Policy Statement on Deception).
- "Consumers should be able to tell when a message comes to them as a paid advertisement. Only then can they evaluate the message critically."[1]

Special feature brought to you by NCSS SASW

CAREER GLIMPSE

Pay It Forward

Having benefited from a strong social support network when he was growing up, Fareez today chooses to excel in a meaningful profession, coming full circle as a social worker.

SHERALYN TAY

The appreciation and the smiles from my clients and the resilience I see in them keeps me going.

For career details: socialworker.sg

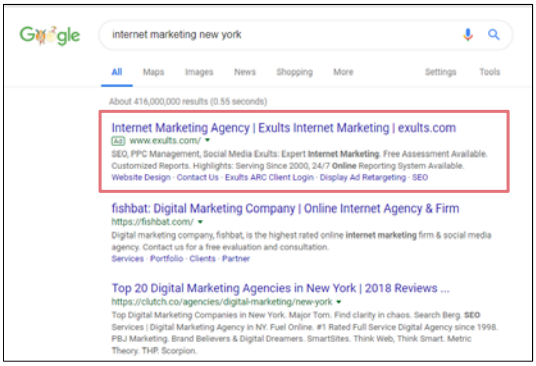
[1] https://www.ftc.gov/public-statements/1996/11/developments-consumer-protection-federal-trade-commission-achieving

4

KILPATRICK TOWNSEND

Paid Search Results

- In the early 2000s, FTC turned its eye toward paid search results.
- In 2002, FTC declined to take formal action against search engines, but recognized "the need for clear and conspicuous disclosures of paid [search] placement, and in some instances paid inclusion."[1]



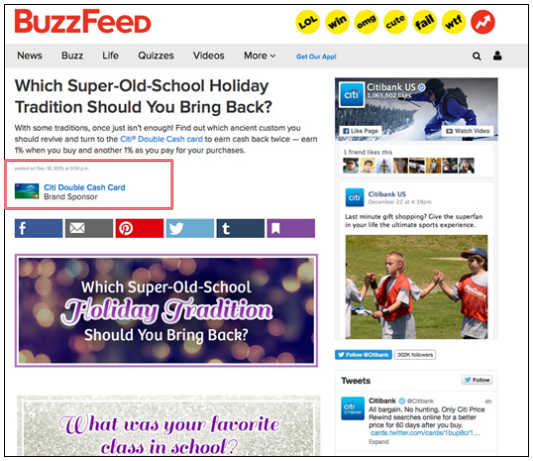
[1] https://www.ftc.gov/sites/default/files/documents/closing_letters/commercial-alert-response-letter/commercialalertletter.pdf

5

KILPATRICK TOWNSEND

Sponsored Content & Native Ads

- Ads formatted to match the style of surrounding content.
- In its December 2015 Policy Statement on Deceptively Formatted Ads, FTC specifically addressed sponsored content & native advertising. [1]
- FTC paid particular attention to misleading formatting, and misleading source identification.



[1] https://www.ftc.gov/system/files/documents/public_statements/896923/151222deceptiveenforcement.pdf

6

KILPATRICK TOWNSEND

FTC Historical Action

Over the years, the FTC has challenged in this area:

- "advertorials" that appeared as news stories or feature articles,
- direct-mail ads disguised as book reviews,
- infomercials presented as regular television or radio programming,
- in-person sales practices that misled consumers as to their true nature and purpose,
- mortgage relief ads designed to look like solicitations from a government agency,
- emails with deceptive headers that appeared to originate from a consumer's bank or mortgage company
- paid endorsements offered as the independent opinions of impartial consumers or experts.

7

KILPATRICK TOWNSEND

FTC Endorsement Guides

FTC Endorsement Guides

- "Advertising" includes social media
- Disclose Material connections between advertiser and influencers
- Expanded liability for advertisers and endorsers
- Advertiser obligated to monitor

8

KILPATRICK TOWNSEND

FTC Endorsement Guides

MATERIAL CONNECTIONS

Disclose any MATERIAL CONNECTION with influencer

- **"material connection"** =
  - Incentives e.g. free swag, prizes, special access, privileges
  - Relationship with advertiser - employment
- Disclosure must Clear and Conspicuous; easily understood; unambiguous

9

KILPATRICK TOWNSEND

FTC Endorsement Guides

It's Real Money

May 9, 2018:

- **Dwayne "The Rock" Johnson is charging Universal Pictures $1 million to promote his upcoming film "Red Notice" on his own social media pages, according to Variety.**
- **The million-dollar "social-media fee" is part of his $22 million salary for the film, which is second only to Daniel Craig's $25 million salary for the upcoming "James Bond" film, according to Variety's round-up of high-profile film salaries.**
- **Johnson currently stands at 105.6 million followers on Instagram, 57.7 million on Facebook, and 12.9 million on Twitter.**

10

KILPATRICK TOWNSEND

FTC Endorsement Guides

FTC v. CSGO Lotto: Sept. 2017

- Settlement with 2 influencers
- Who also owned the company
- Posted promoting “Counter-Strike: Global Offensive” video game
- Never disclosed they actually owned the company that produced the video game
- Also paid other influencers $2,500-$55,000 to promote game, but contractually prohibited influencers from saying anything negative about it
- Same Day: FTC announced having sent 21 influencers warning letters for failing to disclose material connections.

11

KILPATRICK TOWNSEND

Influencer & Endorser Policy Guidance

DO

- Place disclosures up front (before users can click on, watch or read the sponsored content) in the main communication. See: Platform Specific Placement Guidance chart page 2.
- Craft your disclosure for the intended audience.
- Use a larger font or repeat disclosures on lengthy posts or if the content includes repeated claims.

DON’T

- Require additional action, such as scrolling, to see the disclosure.
- Place the disclosure on a busy screen or moving background where it may be difficult to see.
- Rely on the placement of a disclosure in a hyperlink, page description or profile to provide your notice.

12

KILPATRICK TOWNSEND

Platform-Specific Disclosure Placement Guidance	
Platform	**Placement**
Twitter	- Disclosure must appear in first 90 characters of copy, prior to any links or other #s, and must be visible to viewers without any additional action across all devices.
Facebook & Instagram	- Paid Partnership or Sponsored Tag mechanism must be supplemented with a # or plain language disclosure. - Disclosure must appear in first 90 characters, prior to any links or other #s, and must be visible to viewers without any additional action across.

SnapChat	- Disclosure must appear on screen in each snap. Disclaimer placement on screen and choice of font size/ style/ color should ensure that the disclaimer is easy to notice and read.
	- Exceptions:
	  - Disclosure may be given verbally if the endorsement is also only provided verbally (no images, visual references to the product/ brand/ campaign/ Unilever on screen).
	  - No disclosure necessary for Influencer takeovers of a Brand's SnapChat account.

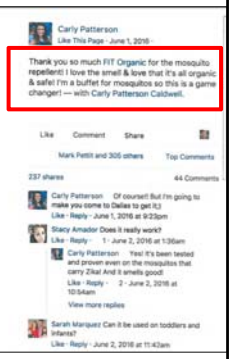
Pinterest	- Disclosure must appear in the main communication, prior to clicking.
Blogs	- Disclosure must be provided at the beginning of the post, prior to any mention of Unilever, brand, product or campaign. - Any social media communication notifying followers of a new blog post must also include a # or plain language disclaimer acknowledging the relationship to Unilever or the brand.
YouTube & Other Videos	- Must appear in the video description AND either: on-screen (placement, font style/size and length of time on screen should ensure that the disclaimer is easy to notice and read), OR, verbally as part of the script introduction; - Must appear prior to any reference to the brand/ product/ campaign/ Unilever; - If the video is long and the brand/ product/ campaign reference does not happen until later in the video the notice of the connection should be repeated, either on screen or verbally in the script.
Streaming	- Disclosure must appear several times on-screen to ensure that viewers see the disclosure no matter when they begin streaming. - Placement, font style/size and length of time on screen should ensure that the disclaimer is easy to notice and read.

Helpful Resources: The FTC has issued the following guides regarding social media activities on behalf of brands by influencers and endorsers. Please review and familiarize yourself with (and follow!) these guides. The FTC's Endorsement Guides: https://www.ftc.gov/system/files/documents/plain-language/pdf-0205-endorsement-guides-faqs_0.pdf. Guides Concerning the Use of Endorsements & Testimonials in Advertising: https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-publishes-final-guides-governing-endorsements-testimonials/091005revisedendorsementguides.pdf

13

KILPATRICK TOWNSEND

FTC Complaint against PR firm Creaxion Corporation and specialty sports magazine publisher Inside Publications



Endorsements did not disclose Carly Patterson or Jake Dalton's paid promotional relationship with HealthPro

14

KILPATRICK TOWNSEND

Short form disclosure options: #Paid, #Sponsor, #Ad, #FITOrganicPartner, #FITOrganic Ambassador

Plain language disclosure options: "I've partnered with FIT Organic to . . ." "So excited to work with FIT Organic on . . ." "Proud to be a part of the most recent FIT Organic campaign . . ."

15

KILPATRICK TOWNSEND

Inside Publications posted and reposted statements on social media about FIT Organic Mosquito Repellent, primarily through its *Inside Gymnastics* accounts.

Inside Publications did not disclose the spokespersons' paid promotional relationships with HealthPro or that its own statements were paid commercial advertising.

Short form disclosures: #paid, #sponsor, #ad

16

KILPATRICK TOWNSEND

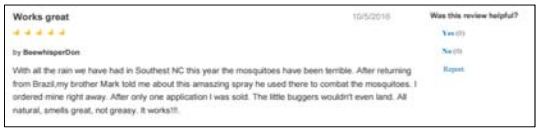
Inside Gymnastics magazine published articles referring to FIT Organic Mosquito Repellent. The articles did not disclose they were paid commercial advertising.

Disclosure options if the advertiser created the content: "Paid Advertisement," "Advertisement"

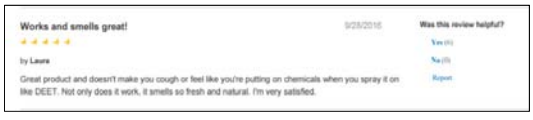
Disclosure options if the advertiser funded but did not create the content: "Sponsored by FIT Organic," "Brought to you by FIT Organic," "Made possible by FIT Organic"

17

KILPATRICK TOWNSEND


Works great
10/5/2016
Was this review helpful?
by BeewhisperDon
With all the rain we have had in Southest NC this year the mosquitoes have been terrible. After returning from Brazil,my brother Mark told me about this amaszing spray he used there to combat the mosquitoes. I ordered mine right away. After only one application I was sold. The little buggers wouldn't even land. All natural, smells great, not greasy. It works!!!.


Worked for me in Brazil
9/29/2016
Was this review helpful?
by Mark
I used this product on a recent hike in a Brazilian rainforest and didn't get a single mosquito bite. A fellow hiker had been bitten by several mosquitos. Apparently, the spray he was using did not work. I loaned him my Fit Organic repellent and he loved it. He finished the hike without any more bites. This product smells great and is light on your skin. I highly recommend it.


Works and smells great!
9/28/2016
Was this review helpful?
by Laura
Great product and doesn't make you cough or feel like you're putting on chemicals when you spray it on like DEET. Not only does it work, it smells so fresh and natural. I'm very satisfied.

Creaxion conducted an online consumer review program that reimbursed individuals, including Creaxion employees, for purchasing FIT Organic Mosquito Repellent and posting online reviews.

Reviews did not disclose that the reviewers were reimbursed for buying the product or the reviewers' relationships to the PR and marketing company hired to promote the product.

Short form disclosure options: #FitOrganicEmployee, #lovemyjob **AND** #Got4Free, #FreeProduct, #Free

Plain language disclosure options: "I'd buy this spray even if I didn't work for FIT Organic and got to try the product for free," "So proud to work on a brand that . . . and lets me try the product for free," "My company makes this great product . . ."

18

KILPATRICK TOWNSEND

In regard to the placement of #cirocpartner, the FTC has said that placing a disclosure so far down in the caption of an Instagram post — in this case, on the sixth line — is easy to miss and unlikely to cut it. The disclosure does not even appear without clicking "more."

"Family business!!!" – sufficient disclosure?

TINA.org letter to the FTC asking them to investigate Diageo's use of influencers to market Ciroc Vodka on Instagram.

How often do third party complaints result in regulatory activity at the FTC?

19

KILPATRICK TOWNSEND

DJ Khaled and Floyd Mayweather Jr. settled with SEC – alleged violation of the anti-touting provision of the federal securities laws.

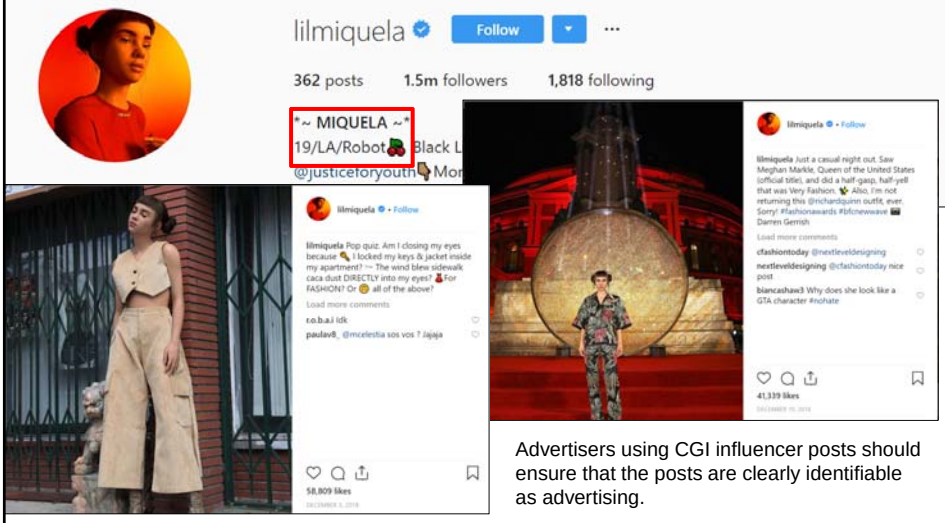
Failed to tell their social media followers that they received money for promoting investments in Initial Coin offerings ("ICOs").

Examples:

- DJ Khaled received a $50,000 payment referring to Centra's ICO as a "Game changer" on various social media accounts.
- Mayweather received a $300,000 payment tweeting that Centra's ICO "starts in a few hours. Get yours before they sell out, I got mine . . ."
- Mayweather allegedly failed to disclose his relationship with two other ICOs that paid him $200,000 for posts such as, "You can call me Floyd Crypto Mayweather from now on."

20

KILPATRICK TOWNSEND



Advertisers using CGI influencer posts should ensure that the posts are clearly identifiable as advertising.

21

KILPATRICK TOWNSEND

Blurring of Ads and Content in the Kids' Space

- *Kids can't differentiate between programs and commercials…*
- Birth of KIDVID
- FCC requires separations between programs and ads
- FTC requires clear and conspicuous disclosures in advertising
- Enforced by Children's Advertising Review Unit (CARU), self-regulatory industry watchdog

22

KILPATRICK TOWNSEND

FTC Disclosures in Sponsored Content, Advertising, Social Influencers

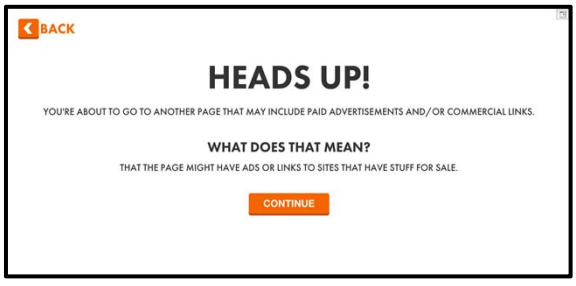
- Persistent visual ad-marking
- Bookend with sponsorship messaging
- Unboxing disclosures - CARU EvanTube Case
- Social influencers with kid followers

23

KILPATRICK TOWNSEND

Persistent Visual Ad-Marking

Internal Bumper



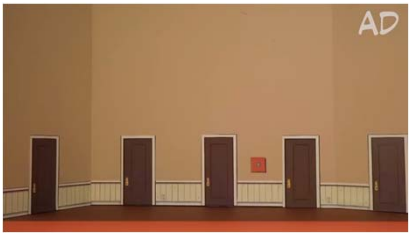
Nick.com

24

KILPATRICK TOWNSEND

Persistent Visual Ad-Marking

Nick Jr. YouTube
(Ad-Marked throughout**)**



Nick YouTube
(Ad-Marked throughout**)**

25

KILPATRICK TOWNSEND

Bookend Sponsorship Messages

Influencer*: Jojo Siwa*

Pikmi Pops Sponsorship

26

KILPATRICK TOWNSEND

YouTube Videos – Unboxing

EvanTubeHD
Disney LEGO without
Sponsorship Disclosure

EvanTubeHD
Mattel Sponsorship Disclosure

KILPATRICK TOWNSEND

YouTube Social Influencers

Influencers*: Eh Bee Family*
Influencers: *Eh Bee Family*
Chrysler Sponsorship Disclosure

Influencers*: Ariel "Baby" Martin & Daniel Skye*
Journeys and Converse
Sponsorship Disclosure

KILPATRICK TOWNSEND

FTC is on the Case

Influencers receiving FTC Warning letters in 2017

1. Naomi Campbell
2. Lindsay Lohan
3. Vanessa Hudgens
4. Snooki (Nicole Polizzi)
5. Sofia Vergara
6. Amber Rose
7. Scott Disick

*(***Doris Day and Chuck Norris did not receive letters)*

29

KILPATRICK TOWNSEND

Advertiser Obligations per the FTC

Advertiser obligations:

- Educate influencers about disclosure req's
- Educate employees/agents
- Require disclosure by influencers
  - *"If you choose to review or share this product please be sure to disclose that it was provided to you by the company."*
- Monitor disclosures
  - Remind and cut off if no compliance

30

KILPATRICK TOWNSEND

Advertiser Obligations per the FTC

FTC says “Everybody knows….” is not true.

FTC says DON’T assume platform disclosure tool is sufficient (e.g. Instagram).

FTC DOES NOT LIKE ambiguous disclosures:

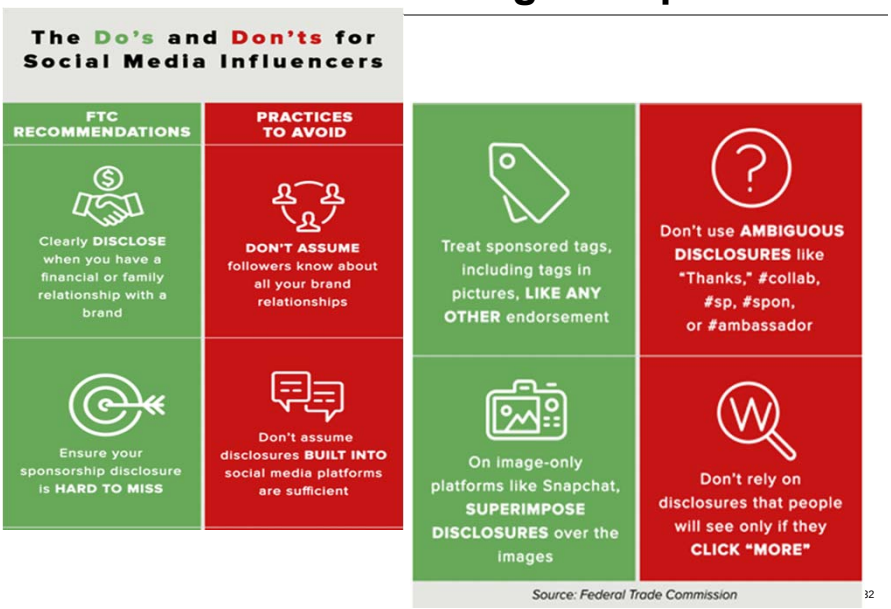
#thanks; #collab; #sp; #spon; #ambassador

FTC says Don’t rely on disclosures only seen if user clicks “more…”

Claim Substantiation concerns still relevant.

KILPATRICK TOWNSEND

Advertiser Obligations per the FTC



KILPATRICK TOWNSEND

Thank you for your time!
Any questions, or comments. . .

33

KILPATRICK TOWNSEND

ANCHORAGE
ATLANTA
AUGUSTA
CHARLOTTE
DALLAS
DENVER
HOUSTON
LOS ANGELES
NEW YORK
RALEIGH
SAN DIEGO
SAN FRANCISCO
SEATTLE
SHANGHAI
SILICON VALLEY
STOCKHOLM
TOKYO
WALNUT CREEK
WASHINGTON D.C.
WINSTON-SALEM

Kilpatrick Townsend & Stockton LLP
The Grace Building | 1114 Avenue of the Americas | New York, NY 10036-7703
212.775.8783

The Media-Content Deal

Marc Lieberstein, Esq.
Kilpatrick Townsend, LLP (Moderator)

David Stonehill, Esq.
SVP & Deputy General Counsel, Global Digital & New Media, Viacom

Rick Baker, Esq.
SVP & Deputy General Counsel, Content Distribution, Viacom

Jill Greenwald, Esq. Assistant Chief Counsel, ABC, Inc.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED FEDERATION OF CHURCHES LLC d/b/a THE SATANIC TEMPLE, Plaintiff, -against- NETFLIX, INC. and WARNER BROS. ENTERTAINMENT INC., Defendants.	Index No. 1:18-cv-10372 **COMPLAINT AND JURY DEMAND**

Plaintiff, United Federation of Churches LLC d/b/a The Satanic Temple ("Plaintiff" or "TST"), by its attorneys, D'Agostino, Levine, Landesman & Lederman, LLP, for its complaint (the "Complaint") against defendant, Netflix, Inc. ("Netflix"), and defendant, Warner Bros. Entertainment Inc. ("Warner Bros."), alleges as follows:

NATURE OF THE ACTION

1. This is an action for copyright infringement, false designation of original, false description; and forbidden dilution under trademark dilution under 15 USC § 1125, and Injury to Business reputation dilution under New York General Business Law § 360-l, all arising out of Warner Bros.'s production and Netflix's distribution of the original Netflix television series known as the *Chilling Adventures of Sabrina* (the "Sabrina Series"), and advertisements thereof, which prominently feature, benefit from and defame TST's unique original expression (the "TST Baphomet with Children") of the historic Baphomet, an androgynous goat-headed deity. Copies of images of the TST Baphomet with Children in its original plater cast form and current bronze casted form are annexed as Exhibits A-1 through A-4 and Exhibit B.

2. This case presents, among other things, a textbook example of the hornbook explanation of copyright protection that copyright law protects unique expressions, but not the ideas themselves. What makes this case particularly striking and significant is that it arises in the context of Defendants who are highly sophisticated media production and distribution companies which blatantly misappropriated Plaintiff's unique expression of an idea even though they have a long history of vigorously protecting their own intellectual property. For example, one of the leading Second Circuit Court of Appeals dealing with copyright protection is *Warner Bros, Inc. v. Gay Toys, Inc.*, 724. F.2d 327 (1983)(involving among other things, Warner Bros.'s objections to "General Lee" symbols on toy cars and the Dukes of Hazard movie). Copies of side by side images of the TST Baphomet with Children and a Netflix scene featuring its copy thereof are annexed as Exhibit C. Copies of screenshots of promotions for the Sabrina Series from YouTube and its Instagram account are annexed as Exhibits D-1 and D-2. Exhibit D-1 is a screenshot from the official trailer of the Sabrina Series entitled "Chilling Adventures of Sabrina | Featurette: Inside the World of Sabrina Spellman [HD] | Netflix. See https://www.youtube.com/watch?v=DLMULlJA0Us.

3. As explained more fully below, Baphomet is a historical deity which has a complex history, having been associated with accusations of devil worship against the Knight Templar. Baphomet historically involved a goat's head (sometimes known as the "Sabbatic Goat") on a female body associated with Lilith, a figure from Jewish mysticism sometimes considered a goddess of the night. The classic visual representation of idea of Baphomet is an image created in or about 1856 by an occult historian Eliphas Levi (the "1856 Baphomet"), which is notable for its use of a seated figure, with exposed large voluptuous female breasts, androgynous arms, a seeming

male lower body and a Sabbatic Goat's head. *Id.* A copy of the historic Levi drawing of Baphomet is annexed as Exhibit E.

4. TST's original expression of Baphomet, i.e., the TST Baphomet with Children, consists of several modifications from the historic expressions of the deity. Those original modifications are: (1) the placement of human children on either side, forming a triangle where (a) the children are male and female, respectively; (b) the children are a young male of African descent and young girl of Anglo-Saxon descent, respectively; (c) the human children are wearing particular clothes, with the girl wearing knee length sleeveless dress with a prominent high waisted sash, and the boy wearing a sports coat, (d) the girl has straight shoulder length hair with exposed ears and the boy has close cropped hair establishing African ancestry, and (2) use of an exposed male chest, instead of exposed large voluptuous female breasts. Importantly, these original expressions are misappropriated through use of an obvious copy which is featured prominently throughout the Sabrina Series and the central focal point of the school in the Sabrina Series which represents evil antagonists.

5. The Sabrina Series depicts the evil antagonists in conformity to the "Satanic Panic" conspiracy theories from the 1980s. See, generally, *Wikipedia* "Satanic ritual abuse" (available at https://en.wikipedia.org/wiki/Satanic_ritual_abuse) (last visited November 7, 2018).

6. The Sabrina Series' evil antagonists stand in stark contrast to TST's tenets and beliefs. See "Tenets," at ¶21, below. By misappropriating TST Baphomet with Children (which is a registered copyright and famous mark of TST) to publish this false and defamatory depiction of TST, Defendants have engaged in three classes of wrong: copyright infringement (Claim 1), trademark violation (Claim 2), and injury to business reputation (Claim 3).

JURISDICTION AND VENUE

7. This action arises under the Copyright Act of 1976 (the "Copyright Act"), 17 U.S.C. §§ 101 *et seq.*, and concerns rights in an original work of authorship over which this Court has original and exclusive subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a), as well as the Lanham Act, 11 U.S.C. § 1125, and also pendent and ancillary claims for Injury to Business Reputation under New York's General Business Law § 360-l.

8. The Court has personal jurisdiction under New York's CPLR § 311 over Netflix because it is a foreign corporation registered to do business in the state of New York, and also because it maintains offices at 245 West 17th Street, New York, NY.

9. The Court has personal jurisdiction under New York's CPLR § 311 over Warner Bros. because it is a foreign corporation registered to do business in the state of New York, and also because it maintains offices at 1325 Avenue of the Americas, New York, NY.

10. Venue is proper in this district pursuant to 28 U.S.C. § 1400(a).

11. Prior to commencing this lawsuit, TST complied with all legal prerequisites. TST registered the TST Baphomet with Children with the United States Copyright Office and been granted registrations VA 2-116-092 and VA 0002124601.

THE PARTIES

12. Plaintiff TST is a Massachusetts limited liability company, with its principal place of business located at 64 Bridge Street, Salem, Massachusetts 01970.

13. Upon information and belief, Warner Bros. is, among other things, a production company of motion pictures and television series.

14. Warner Bros. is the producer of the Sabrina Series.

15. Upon information and belief, Netflix is, among other things, an internet distributor of television series.

16. Netflix is the internet distributor of the Sabrina Series.

FACTUAL ALLEGATIONS

A. Historic Background of Baphomet

17. As indicated above, Baphomet is a goat-headed, angel-winged, hermaphroditic (having both male and female features) deity of antiquity. Baphomet represents a conciliation of opposites. Baphomet is neither human nor beast, neither male nor female, neither angelic nor demonic. Simultaneously, Baphomet is all of these. Baphomet historically was believed to have a Sabbatic Goat's head placed on the body of Lilith, a figure from Jewish mysticism sometimes considered the goddess of the night. Baphomet was first rendered to modern form (See Exhibit E) by Eliphas Levi, an occult historian, in 1856. See *Dogme et Rituel de la Haute Magie* ("Dogma and Rituals of High Magic.") The Knights Templar were falsely accused of worshipping Baphomet and that subsequently became incorporated into various occult and mystical tradition. See, generally, *Wikipedia* "Baphomet" (available at https://en.wikipedia.org/wiki/Baphomet) (last visited November 7, 2018). The 1856 Baphomet is notable for its use of exposed large voluptuous female breasts, androgynous arms, and a seeming male lower body.

B. The Satanic Temple

18. TST is an organization founded and designed to encourage benevolence and empathy among people rejecting tyrannical authority, advocating practical and common-sense justice, and undertaking noble pursuits guided by individual will. Foundational to TST's belief structure is protection of an individual's right to make informed choices of their own free will.

19. TST does not promote evil and instead holds to the basic principle that undue suffering is bad, and that which reduces suffering is good.

20. Satan, for TST, is a literary figure symbolic of the eternal rebel in opposition, rather than the personalization of evil. To TST, "Satan" is the literary Satan, meant to be a rebel against God's authority, rather than an evil being, best exemplified by Milton and the Romantic Satanists, from Blake to Shelley to Antole France.

21. TST believes in the pursuit of knowledge and freedom of will, based upon the following seven (7) tenets.

(a) One should strive to act with compassion and empathy towards all creatures in accordance with reason.

(b) The struggle for justice is an ongoing and necessary pursuit that should prevail over laws and institutions.

(c) One's body is inviolable, subject to one's own will alone.

(d) The freedoms of others should be respected including the freedom to offend. To willfully and unjustly encroach upon the freedoms of another is to forgo one's own.

(e) Beliefs should conform to one's best scientific understanding of the world.

(f) People are fallible. If one makes a mistake, one should do one's best to rectify it and resolve any harm that might have been caused.

(g) Every tenet is a guiding principal designed to inspire nobility in action and thought. The spirit of compassion, wisdom and justice should always prevail over the written or spoken word.

22. TST is politically aware and has, among other things, opposed The Westboro Baptist Church, advocated on behalf of children in public schools to abolish corporal punishment, and has applied for equal representation where religious monuments are place on public property.

23. In connection with its mission, TST believes that the First Amendment of the Constitution of the United States mandates that the United States Government treat all religions equally.

24. TST's Baphomet with Children was designed so that after a statue of the Ten Commandments was donated to Oklahoma City by State Representative Mike Reitze, TST could donate its own unique expression of Baphomet.

C. The Creation of the TST Baphomet with Children

25. In or around 2013/2014, TST's members and managers designed and commissioned, at substantial cost and with great effort and attention to detail, the TST Baphomet with Children.

26. Members and managers of TST initially created a sketch (the "Initial Sketch"), showing a figure somewhat similar to the 1856 Baphomet, but which was configured in a triangular arrangement, with a young girl of apparent Anglo-Saxon descent on the left facing Baphomet and a young boy of apparent African descent on the right facing Baphomet. The idea was to have the children looking reverentially at Baphomet. A copy of the initial sketch is attached as Exhibit F.

27. The TST Baphomet with Children was designed to be an answer to religious display on public property and as an assertion of pluralism and equal status in an environment of religious freedom, all key tenets of TST. See also ¶ 21(b), (d).

28. Each element of the TST Baphomet with Children was carefully and specifically developed from the initial sketch with an artist, commissioned on a work-for-hire basis. Among

other things, numerous child models were considered to find a specific expression of bi-racial childlike innocence by children of different races, looking up in reverence at Baphomet. An affirmative decision was made to put the young boy of African descent into a sports jacket instead of the tee-shirt in the initial sketch and to put the young girl in a sleeveless knee length dress with a high waist sash, rather than the dress with covered shoulders and leggings in the original sketch Additionally, Baphomet's arms, which were originally angled down similar to the 1856 Baphomet, were raised to be a straight and rigid right angles, with prominent muscular biceps. In the 1856 Baphomet, Baphomet's eyes are intense and seem to imply evil; in TST Baphomet with Children, Baphomet's eyes are softened to imply wisdom.

29. TST spent countless number of hours and approximately $100,000 to develop the actual statue which is the now-famous TST Baphomet with Children.

D. Extensive publicity which has made the TST Baphomet with Children a famous symbol of TST

30. The public release of the TST Baphomet with Children has been subject to extensive world-wide publicity and media coverage which has made it a famous symbol of TST.

31. Publicity surrounding the release of the initial drawing, the original plaster cast and the final bronze version, include articles in Time Magazine and The New York Time, as well as pieces on CBS, Fox News, the Colbert Show and Lisa Ling's This is Life on CNN, among others, as follows:

- January 6, 2014
  CBS News and Time Magazine display initial sketch
  https://www.cbsnews.com/news/group-unveils-plans-for-satan-statue-at-okla-capitol/

  http://nation.time.com/2014/01/07/satanists-unveil-statue-for-oklahoma-capitol/

- May 1, 2014
  TST releases the first images of the plaster Baphomet still under construction in a piece for Vice Magazine

https://www.vice.com/en_us/article/xd5gjd/heres-the-first-look-at-the-new-satanic-monument-being-built-for-oklahomas-statehouse

- May 6, 2014

Colbert Report
http://www.cc.com/video-clips/zekn1k/the-colbert-report-satanic-monument-for-the-oklahoma-state-house

https://www.huffingtonpost.com/2014/05/07/stephen-colbert-war-on-religion-america_n_5282574.html

- July 10, 2015

NY Times publishes image of plaster Baphomet (not the first to do so, but a major outlet)
https://www.nytimes.com/2015/07/11/us/a-mischievious-thorn-in-the-side-of-conservative-christianity.html?login=email&auth=login-email

- July 2015

Fox News Video on Detroit unveiling of bronze statue
https://www.dailymotion.com/video/x30r201

- Sept 6, 2015

RT displays plaster Baphomet
https://www.rt.com/usa/314775-arkansas-capitol-satanic-temple/

- November 30, 2015

Lisa Ling, This is Life on CNN (during prime time on Sundays)
https://www.cnn.com/videos/tv/2015/11/30/satanic-temple-lisa-ling-orig.cnn

- November 13, 2015

Raw Story - Plaster Baphomet
https://www.rawstory.com/2015/11/christians-unwittingly-allowed-satanists-to-ambush-missouris-anti-abortion-laws-heres-how/

- August 17, 2016

Arkansas Times - Plaster Baphomet
https://www.arktimes.com/arkansas/the-devil-is-in-the-details-at-the-arkansas-state-capitol/Content?oid=4538981

- November 2, 2016

Boston College student paper - Bronze Baphomet
http://bcheights.com/2016/11/02/reassessing-world-satanic-temple/

- January 25, 2017

Arkansas Times - Plaster Baphomet

https://www.arktimes.com/ArkansasBlog/archives/2017/01/25/site-plan-approved-for-satanic-temple-monument-public-comment-legislative-approval-hurdles-yet-to-be-cleared

- May 2017
Heavy - Plaster Baphomet
Heavyhttps://heavy.com/news/2017/05/satanic-temple-monument-statue-salem-tenents-baphomet-abortion/

- June 28, 2017
Haute Macabre - Bronze Baphomet
http://hautemacabre.com/2017/06/never-let-your-activism-be-artless-an-interview-with-lucien-greaves-of-the-satanic-temple/

32. A YouTube video shows the TST Baphomet with Children as a unique work of art. (See https://www.youtube.com/watch?v=NrnW6-pjQa0).

33. In 2015, coinciding with announcement of TST's intention to donate the TST Baphomet with Children to Oklahoma to be placed alongside the Ten Commandments, the Oklahoma Supreme Court overturned the statutory framework which permitted the Oklahoma Ten Commandments monument. See *Prescott v. Okla. Capitol Pres. Comm'n*, 2015 OK 54, 373 P.3d 1032.

34. Following that, TST Baphomet with Children was repurposed to be paired with a then-proposed Ten Commandments monument in Arkansas. Litigation in Arkansas is ongoing. See Cave v. Martin, (4:18-cv-00342) (E.D. Ark.).

35. TST's website, at all relevant times, explained that TST's Baphomet with Children was a unique expression, noting that TST Baphomet with Children has a "male chest" and picturing Baphomet with two children, a small boy and small girl, looking up at the Sabbatical Goat head of the statute. TST's website further explains that the TST Baphomet with Children is on display in an art gallery and is being offered to other states where a religious statute appears on publicly-owned land. TST's website explains the relationship of the TST Baphomet with Children to the

First Amendment mission of TST to ensure that government treats all religions equally. A copy of the Baphomet page of TST's website is attached as Exhibit G.

36. Partly due to the extensive broadcasted depictions of TST Baphomet with Children, both bronze-cast and plaster-cast, as well as the efforts of TST to publicize its mission in connection with the TST Baphomet with Children, this statue has become a famous mark which is inextricably linked with TST.

E. The Sabrina Series

37. The Sabrina Series is a fictional television series based upon issues of magic and mischief colliding as a half-human, half-witch teenager named Sabrina navigates between two worlds: mortal teen life and her family legacy, the Church of the Night.

38. This series was produced by Warner Bros. and distributed by Netflix. The Sabrina Series was released to the public on October 26, 2018.

39. Shortly prior to airing, featurettes and advertisements were circulated on public media, such as YouTube and Instagram. Upon information and belief, these advertisements included the misappropriated TST Baphomet with Children, such as the image on Exhibits D-1 and D-2.

40. Defendants misappropriated the TST Baphomet Children in ways implying that the monument stands for evil. Among other morally repugnant actions, the Sabrina Series' evil antagonists engage in cannibalism and forced-worship of a patriarchal deity.

41. The TST Baphomet with Children appears in at least 4 of the 10 episodes of the Sabrina Series, and numerous scenes.

42. Defendants feature the TST Baphomet with Children as a central figure for the antagonists. In Episode 2 of the Sabrina Series, TST Baphomet with Children is unveiled as a

foreboding figure and the focal point of the Witches Academy. In the final scene of the series at the end of Episode 10, the main character walks in front of TST Baphomet with Children, rendering it a key element of the season finale.

43. Comparison of the parties' statues, as show in Exhibit C, demonstrates that the unique elements of TST's expression of the idea of Baphomet, and particularly the use of a male chest rather than voluptuous large female breasts, and the configuration with a small boy and small girl looking at the Sabbatic Goat head of the statue, were unquestionably copied by Defendants. The similarities are no coincidence. Also, compare Exhibit A-1 with Exhibit D-1.

44. By notice dated October 26, 2018, Defendants were notified of copyright violations inherent in Netflix's use of the TST Baphomet with Children. Defendants have not responded.

45. Defendants brazenly ignored TST's demands, thereby forcing TST to file suit to protect its intellectual property rights.

46. Defendants' unauthorized reproduction and distribution of the Sabrina Series and advertising thereof has harmed and, if not permanently enjoined, will continue to harm the commercial value of TST's copyrighted work and the rights of ownership and control which TST enjoys in the TST Baphomet with Children.

47. TST seeks, among other things, a permanent injunction barring Defendants from reproducing and distributing the Sabrina Series utilizing images of the TST Baphomet with Children, and TST submits that absent the relief requested herein, Defendants will continue to willfully infringe TST's copyright, trademark and common law rights.

F. Defendants' cavalier disregard to TST's property rights

48. TST's objection to the Sabrina Series' blatant misappropriation of the TST Baphomet with Children was, among other places, reported in VICE, a news media organization,

on October 29, 2018. See https://broadly.vice.com/en_us/article/zm9pe3/satanic-temple-claims-netflixs-sabrina-illegally-copied-baphomet-statue (Last visited November 7, 2018). There, Lisa Soper (the production designer for the Sabrina Series) spoke about the statue and falsely stated, "I think that's kind of a coincidence." Going further, "When you look at Baphomet, there's really only a couple of statues of him—which, they have their statue, and we've got our statue in the show." "If you look at Goya paintings, if you look at a lot of the tarot cards, or the Alistair Crawley iterations of him—because there's hundreds and hundreds of iterations of him, he's always seen with his people around him and it's more of like a father figure kind of thing. So depicting his children with him, that kind of stuff, and those kinds of elements are all kind of the same." Soper further said: "But it's no different from, in my opinion anyhow... from any other of the mass amounts of iterations of him that have been around."

49. The above is demonstrably false. Upon information and belief, Baphomet has never been depicted with two children gazing reverentially at the Sabbatic Goat head. Likewise, upon information and belief, Baphomet, prior to TST's Baphomet with Children depictions generally include large exposed large voluptuous female breasts, not a male chest. The female breasts are a central feature of the traditional depiction of Baphomet, the *hermaphroditic* deity.

50. Ms. Soper's statement is a bold lie. That lie was designed to further damage TST and promote the Sabrina Series at the expense of TST and its business reputation.

FIRST CLAIM FOR RELIEF
(Copyright Infringement)

51. Plaintiff repeats and realleges each and every allegation contained in paragraphs 1 through 50 above as if fully set forth herein.

52. The TST Baphomet with Children is an original work of authorship and is copyrightable under the laws of the United States.

53. TST is the holder of US Copyright registrations VA 2-116-0092 and VA 002124601 for the TST Baphomet with Children.

54. The TST Baphomet with Children is the, "most politically charged sculpture of our time." See Exhibit G. See also https://salemartgallery.com/baphomet/. This puts the public, specifically Defendants, on reasonable notice of intellectual property issues and that the TST Baphomet with Children is a unique work of art that should not be misappropriated as a symbol of evil.

55. Plaintiff has not assigned, licensed, or otherwise transferred any of its exclusive rights to Defendants or made them available for public use.

56. Defendants are unlawfully reproducing, distributing, and selling copies of the Sabrina Series, including advertisements thereof which include unauthorized use of the TST Baphomet with Children, without authorization. This violates Plaintiff's exclusive intellectual property rights.

57. Defendants are aware that they do not have permission to reproduce, distribute, or sell copies of television series featuring of the TST Baphomet with Children.

58. By failing or refusing to take down the misappropriated imagery, Defendants are willfully infringing upon Plaintiff's copyright.

59. Based upon the foregoing, Plaintiff is entitled to a judgment against Defendants in an amount to be determined at trial, but believed to be no less than $50,000,000.00, together with injunctive relief.

SECOND CLAIM FOR RELIEF
(False designation of original, false description; and forbidden dilution under trademark dilution under 15 USC 1125)

60. Plaintiff repeats and realleges each and every allegation contained in paragraphs 1 through 59 above as if fully set forth herein

61. The TST Baphomet with Children is a symbol of TST.

62. The TST Baphomet with Children is a famous mark, within the meaning of 15 USC § 1125 (c).

63. Defendants have used the TST Baphomet with Children in ways that falsely designate its origin and are misleading and false to the extent that the Sabrina Series indicates, impliedly and expressly, that the TST Baphomet with Children is a symbol of evil, associated with forced-devil worship, cannibalism, and murder.

64. Among other things, TST designed and commissioned the TST Baphomet with Children to be a central part of its efforts to promote First Amendment values of separation of church and state and equal protection. Defendants' prominent use of this symbol as the central focal point of the school associated with evil, cannibalism and murder blurs and tarnishes the TST Baphomet with Children as a mark of TST.

65. Defendants have used the TST Baphomet with Children in ways that causes caution by blurring or diluting by tarnishment as a symbol of TST.

66. Defendants' use of the TST Baphomet with Children has injured and continues to injure Plaintiff.

67. Based upon the foregoing, Plaintiff is entitled to a judgment against Defendants in an amount to be determined at trial, but believed to be no less than $50,000,000.00, together with injunctive relief.

THIRD CLAIM FOR RELIEF
(Injury to Business reputation dilution under New York General Business Law § 360-l)

68. Plaintiff repeats and realleges each and every allegation contained in paragraphs 1 through 67 above as if fully set forth herein.

69. Defendants have used images of the TST Baphomet with Children in a way that injures the business reputation of TST and dilutes the distinctive quality of the TST Baphomet with Children as a mark of TST in violation of New York's General Business Law Section 360-l.

70. Among other things, TST designed and commissioned the TST Baphomet with Children to be a central part of its efforts to promote First Amendment values of separation of church and state. Defendants' prominent use of it as the central focal point of the school associated with evil, cannibalism and possibly murder is injurious to TST's business.

71. Defendants' use of the TST Baphomet with Children has injured and continues to injure Plaintiff.

72. Based upon the foregoing, Plaintiff is entitled to a judgment against Defendants in an amount to be determined at trial, but believed to be no less than $50,000,000.00, together with injunctive relief.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff demands the following relief:

(a) An order declaring that Defendants are liable for infringement of TST's copyright in and to the TST Baphomet with Children;

(b) An order declaring that Defendants have willfully infringed Plaintiff's copyright in and to the TST Baphomet with Children;

(c) An order pursuant to 17 U.S.C. § 504, awarding Plaintiff monetary damages for copyright infringement, in an amount to be established at trial but believed to exceed $50,000,000.00 consisting of: (i) actual damages, in an amount to be determined at trial, along with disgorgement of all of Netflix's profits attributable to sales of the Sabina Series; or, (ii) in the alternative, statutory damages, in an amount to be determined at trial, arising from Defendants' willful copyright infringement;

(d) An order enjoining Defendants from any future reproduction or distribution of the Sabrina Series with the TST Baphomet with Children and requiring Defendants to digitally remove the TST Baphomet with Children from all future distributions of the Sabrina Series and to cease and desist all marketing of the Sabrina Series which uses the images of the TST Baphomet with Children and to deliver the TST Baphomet with Children to the Plaintiff;

(e) An order pursuant to 17 U.S.C. § 505, awarding Plaintiff the recovery of attorneys' fees, interest and costs;

(f) An order declaring that Defendants are liable for false designation of original, false description and forbidden dilution under trademark dilution under 15 USC § 1125;

(g) An order pursuant to 15 U.S.C. 1125, awarding Plaintiff monetary damages in an amount to be established at trial but believed to exceed $50,000,000.00 and an injunction for false designation of original, false description and forbidden dilution under trademark dilution;

(h) An order pursuant to New York General Business Law § 360-l declaring that Defendants are liable for injury to business reputation and dilution of a mark;

(i) An order pursuant to New York General Business Law § 360-l, awarding Plaintiff monetary damages in an amount to be established at trial but believed to exceed $50,000,000.00 and an injunction for liable for injury to business reputation and dilution of a mark;

(j) Reimbursement of attorneys' fees, costs and disbursements.

(k) Such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, the Plaintiff demands trial by jury in this action of all issues so triable.

Dated: November 8, 2018

D'Agostino, Levine, Landesman &
Lederman, LLP

By: /s/
Bruce H. Lederman, Esq.
Attorneys for the Plaintiff
345 Seventh Ave., 23rd Floor
New York, New York 10001
Tel: (212) 564-9800
Fax: (212) 564-9802

ORIGINAL

BROWNE GEORGE ROSS LLP
Eric M. George (State Bar No. 166403)
egeorge@bgrfirm.com
Jeffrey C. Berman (State Bar No. 308500)
jberman@bgrfirm.com
2121 Avenue of the Stars, Suite 2800
Los Angeles, California 90067
Telephone: (310) 274-7100
Facsimile: (310) 275-5697

Attorneys for Plaintiffs Hofflund/Polone and Gavin Polone

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

BC 698058

HOFFLUND/POLONE, a California partnership, and GAVIN POLONE, an individual,

Plaintiffs,

vs.

WARNER BROTHERS ENTERTAINMENT, INC., TIME WARNER ENTERTAINMENT COMPANY, L.P.; WARNER BROS. TELEVISION PRODUCTION, INC.; WB STUDIO ENTERPRISES, INC.; THE WB TELEVISION NETWORK PARTNERS, L.P.; WB COMMUNICATIONS, INC.; THE CW NETWORK, LLC; WARNER BROS. ENTERTAINMENT, INC.; TIME WARNER, INC.; AND DOES 1-10,

Defendants.

Case No.

COMPLAINT FOR:

1. **BREACH OF CONTRACT**
2. **BREACH OF FIDUCIARY DUTY**
3. **BREACH OF THE COVENANT OF GOOD FAITH AND FAIR DEALING**
4. **FRAUD**
5. **NEGLIGENT MISREPRESENTATION**
6. **UNFAIR BUSINESS PRACTICES**
7. **UNLAWFUL TYING AGREEMENT**
8. **ACCOUNTING**
9. **CONSTRUCTIVE TRUST**

DEMAND FOR JURY TRIAL

Plaintiffs Hofflund/Polone and Gavin Polone allege as follows:

INTRODUCTION

1. Television and movie producer Gavin Polone and writer Amy Sherman-Palladino developed and produced *Gilmore Girls* – a hugely successful television show, both artistically and financially. The show, produced in conjunction with Warner Bros. Television Production, Inc., aired on the WB Network for eight years, and has just recently been reprised with the original cast on Netflix as *Gilmore Girls: A Year In the Life*. Time Magazine named *Gilmore Girls* one of the top 100 series of all time.

2. Unfortunately, Warner Bros. has not been willing to share the financial benefits flowing from *Gilmore Girls* and *Gilmore Girls: A Year in the Life* in a fair, equitable, or contractually-mandated fashion. Indeed, Mr. Polone repeatedly has been forced to take Warner Bros. and its affiliated companies to court to seek a just distribution of the shows' financial rewards. After years of stonewalling in response to Mr. Polone's latest efforts at economic and contractual justice, the Warner Bros. parties have forced Mr. Polone to seek judicial intervention once more.

3. In particular, Defendants Warner Brothers Entertainment, Inc.; Time Warner Entertainment Company, L.P.; Warner Bros. Television Production, Inc.; WB Studio Enterprises, Inc.; The WB Television Network Partners, L.P.; WB Communications, Inc.; The CW Network, LLC; Warner Bros. Entertainment, Inc.; and Time Warner, Inc. (collectively, "Defendants") have willfully avoided paying Hofflund/Polone and Mr. Polone (together, "Plaintiffs") the full share of revenues to which they are entitled based on the terms of agreements between Mr. Polone, through himself and his loan out entity Hofflund/Polone, on the one hand, and Defendants on the other.

4. This case is part of a long and troubled line of successful artists of all stripes being forced to seek recourse in court against a corporate producing partner that manipulates its back room accounting and distorts the interpretation of its contractual obligations. The victims of this oppressive behavior are the artists who create the content those corporate producing partners exploit on television, at the movie theatre, and more recently on-line. Here, Defendants have used various improper accounting practices to improperly manipulate the profitability of *Gilmore Girls*

and *Gilmore Girls: A Year In The Life* by: (1) erroneously applying – sometimes multiple times – deductions to gross receipts for items not covered under the parties' agreements, such as video expenses, indirect overhead expenses, electronic sell-through, video-on-demand, and subscription video-on-demand ("SVOD") distribution fees for first runs of *Gilmore Girls: A Year In The Life*; (2) charging production costs attributable to shows other than *Gilmore Girls* or *Gilmore Girls a Year in the Life*; (3) engaging in self-dealing by overstating production costs payable to affiliated entities, resulting in artificially reduced profitability; and (4) deferring and holding back cash receipts. By engaging in these willful and wrongful acts, Defendants inflated their own profits by diverting to themselves compensation rightfully due to Plaintiffs.

5. Defendants have also utilized the anticompetitive practice of "straight-lining" – allocating the same portion of the licensing fee to every movie or television show in a package without regard to the true value of each television show or film, which deprives profit participants of a fair allocation of the licensing fees to which they are entitled – and failing to provide a complete reporting for domestic and foreign television sales collections relating to output and package sales. These practices constitute breaches of Defendants' contractual obligations and their duty to act in good faith towards profit participants.

6. When Plaintiffs challenged Defendants' improper practices through their ordinary audit process, Defendants resorted to delay, avoidance and misdirection in an effort to conceal their misconduct. This action seeks to protect and ensure Plaintiffs' rights to the profits due.

PARTIES

7. Plaintiff Gavin Polone is a successful film and television writer, producer, and manager. He is the executive producer of the popular and successful television series *Gilmore Girls*. Mr. Polone has produced many successful films, including *Panic Room*, *Zombieland*, and *A Dog's Purpose* and was an executive producer on the HBO television series *Curb Your Enthusiasm*. Mr. Polone is, and at all times relevant hereto was, an individual residing and doing business in the County of Los Angeles, State of California.

8. Plaintiff Hofflund/Polone is a loan out partnership entity, which provides the professional services of Mr. Polone. Hofflund/Polone is, and at all times relevant hereto was, a partnership doing business in Los Angeles County, California.

9. Defendants are well-known entertainment companies with a pervasive presence in the film production and distribution industry.

10. On information and belief, Defendant Warner Brothers Entertainment, Inc. is, and all times relevant hereto was, a corporation formed under the laws of the State of California and has its headquarters and principal place of business in the County of Los Angeles, State of California.

11. On information and belief, defendant Time Warner Entertainment Company, L.P. is, or was, a limited partnership organized under the laws of the State of Delaware and doing business in Los Angeles County, California.

12. On information and belief, defendant Warner Bros. Television Production, Inc. is, or was, a corporation organized under the laws of the State of Delaware and doing business in Los Angeles County, California. On information and belief, Warner Bros. Television Production, Inc. is, or was, a successor in interest to Time Warner Entertainment Company, L.P.

13. On information and belief, defendant WB Studio Enterprises, Inc. is, or was, a corporation organized under the laws of the State of Delaware and doing business in Los Angeles County, California. On information and belief, WB Studio Enterprises, Inc. is, or was, the successor in interest to Warner Bros. Television Production, Inc.

14. On information and belief, The WB Television Network Partners, L.P. ("The WB Network) is, or was, a limited partnership doing business in Los Angeles County, California. On information and belief, the general partner of The WB Network is, or was, WB Communications, Inc. ("WB Communications"), a California corporation, and the limited partner is, or was, Tribune Broadcasting. On information and belief, WB Communications, Inc. was owned by or was a division of Time Warner Entertainment Company, L.P. until approximately 2003, and thereafter was a subsidiary of Time Warner, Inc.

15. On information and belief, The CW Network, LLC ("The CW Network") is, or was, a limited liability company organized under the laws of the State of Delaware and doing business in Los Angeles County, California. On information and belief, The CW Network is the successor in interest to The WB Network. On information and belief, The CW Network is a joint venture owned 50% by CBS Corporation and 50% by Warner Bros. Entertainment, Inc.

16. On information and belief, some or all of the foregoing entities are, or were, owned (in whole or in part) or affiliated with defendants Warner Bros. Entertainment, Inc. ("WBE") and/or Time Warner, Inc. ("Time Warner"). Time Warner is among the largest conglomerates in the world and bills itself as "a leading media and entertainment company, whose businesses include interactive services, cable systems, filmed entertainment, television networks and publishing." On information and belief, defendants Time Warner and WBE are, or were, corporations organized under the laws of the State of Delaware, and doing business in Los Angeles County, California.

17. Plaintiffs are informed, believe, and thereon allege, that Does 1 through 10, inclusive, are parents, subsidiaries, sister companies, affiliates, agents or representatives of the named defendants and that each Doe defendant is responsible in some manner for the actions herein alleged. The true names and capacities, whether individual, corporate, associate or otherwise, of defendants Does 1 through 10, inclusive, and each of them, are unknown to Plaintiffs at this time, and Plaintiffs therefore sue said defendants by such fictitious names. Plaintiffs will seek leave of court to replace the fictitious names of these entities with their true names when they are discovered.

JURISDICTION AND VENUE

18. This Court has jurisdiction over this matter pursuant to the California Constitution, Article XI, Section 10 and California Code of Civil Procedure §410.10, because Defendants transacted business and committed the acts complained of herein in California. Defendants are located in California, and have their principal places of business in and are headquartered in California.

19. Venue is proper in Los Angeles County pursuant to California Code of Civil Procedure § 395 and because many of the acts complained about occurred in Los Angeles County and Mr. Polone resides in Los Angeles County.

STATEMENT OF FACTS

A. Defendants Have a History of Failing to Make Payments Due to Plaintiffs with Respect to Mr. Polone's Role as Executive Producer of *Gilmore Girls*.

20. On February 16, 2000, Plaintiffs entered into an agreement (the "Series Agreement") with Defendant Warner Brothers Television Production, Inc. to provide executive producer services for a television project called *Gilmore Girls*. The project became an extremely popular television series that aired on primetime television for seven seasons.

21. The Series Agreement required participation payments to be made to Plaintiffs in the amount of 11 ¼ percent of the modified adjusted gross revenue (the "MAGR") of *Gilmore Girls*. Several disputes have arisen between the parties due to Defendants' failure to make payments to Plaintiffs under the Series Agreement.

22. The first dispute related to the Series Agreement arose due to Defendants wrongfully granting favorable terms to affiliated networks for repeat airings of episodes of *Gilmore Girls*, which resulted in less amounts payable to Plaintiffs. The dispute was settled in October 2002 and resulted in modified terms to the Series Agreement, which were more favorable to Plaintiffs (the "Modification Agreement"). Pursuant to the Modification Agreement, the parties agreed, *inter alia*, to increase Plaintiffs' profit participation percentage from 11 ¼ to 12 ½ percent. The parties also agreed to incorporate the Modification Agreement into the Series Agreement.

23. The second dispute between the parties arose in late 2007 pertaining to payments during the period through June 30, 2006, this time regarding license fees payable under the Series Agreement. This action, LASC Case No. BC404543 (the "Second Dispute"), was settled in or about October 2009 following a forensic audit, which revealed numerous errors and omissions in Defendants' accounting to Plaintiffs and resulted in significant sums due and paid to Plaintiffs.[1]

[1] The Second Dispute alleged claims for breach of fiduciary duty, aiding and abetting breach of

24. On or about July 29, 2014, Plaintiffs performed a second audit for the period of April 1, 2009 through September 30, 2011, the findings of which are reflected in an audit report dated July 29, 2014 (the "2014 Audit Report"). The 2014 Audit Report revealed the following discrepancies, which resulted in gross underreporting of amounts (totaling more than $1 million) owing to Plaintiffs:

- Unreported income from home video and electronic sell-through receipts;
- improper deductions of home video placement, legal, and guild/union/residual fees, as well as duplicated distribution expenses; and
- interest payable on the underreported amounts.

25. On or about December 21, 2015, given the success of *Gilmore Girls*, Defendants entered into an agreement with Netflix to revive the series with new episodes under the name *Gilmore Girls: A Year in the Life* (the "Subsequent Episodes").

26. For a third time, Plaintiffs were forced to litigate their rights related to the revival of *Gilmore Girls* under the Series Agreement. That dispute, LASC Case No. BC616555 (the "Third Dispute"), was filed on or about April 8, 2016 and settled on or about October 13, 2016.[2] The Third Dispute also resulted in significant additional monies paid to Plaintiffs.

27. The Third Dispute concerned Defendants' refusal to compensate plaintiff in any way for the Subsequent Episodes. Defendants argued that the Subsequent Episodes did not fall under the terms of the Series Agreement, making the absurd claim that the Subsequent Episodes are *derivative* works based on the television series *Gilmore Girls*.[3]

---

fiduciary duty, breach of contract, breach of the covenant of good faith and fair dealing, inducing breach of contract, intentional interference with contract, accounting, and unfair business practices.

[2] The Third Dispute alleged a breach of contract claim.

[3] The Subsequent Episodes are, and have been widely described in the press as, a "revival" of the series Gilmore Girls. The Subsequent Episodes reintroduced the original program's storyline, characters, and locales. They picked up from where the last episode left off, or at some time after that point. Indeed, the Subsequent Episodes have been widely referred to by fans and the media as the eighth season of the series.

28. Defendants also appeared to erroneously believe the Subsequent Episodes are not considered a "television series" because they were being produced for Netflix, rather than a traditional broadcast network.[4]

29. Defendants abandoned their position on the derivative work and Netflix arguments resulting in an agreement that Defendants shall treat participation payments and all contingent compensation for *Gilmore Girls: A Year in the Life* subject to the terms of the Series Agreement.

B. Defendants' Continued to Engage in Improper Accounting and Business Practices.

30. This is the *fourth* dispute between the parties relating to the Series Agreement and participation payments due to Plaintiffs for *Gilmore Girls* and *Gilmore Girls: A Year in the Life*, reflecting a pattern of Defendants' continued employment of improper accounting practices, despite having clear notice that they were violating Plaintiffs' rights.

31. On or about January 25, 2018, pursuant to the settlement of the Third Dispute, Defendants began making participation payments to Plaintiffs for receipts generated by the Subsequent Episodes of *Gilmore Girls: A Year in the Life*.

32. Defendants improperly applied to these payments a 10 percent distribution fee on first run pay television SVOD runs of Subsequent Episodes. This distribution fee resulted in a nearly two million dollar decrease in the MAGR, thus reducing profit participation payments due Plaintiffs.

33. The SVOD distribution fee is not an allowable fee under the Series Agreement. The SVOD distribution fee is also not a standard expense taken in the industry and has not been applied between the parties in prior dealings. By applying the SVOD distribution fee, Defendants breached their contractual obligations to Plaintiffs.

34. Additional examples of Defendants' improper accounting practices include:

- Improperly manipulating gross receipts by adding improper deductions; omitting

[4] Netflix describes itself on its website as "the world's leading Internet television network." Netflix series have been eligible to compete in the best television series award categories since as far back as 2008.

deferring, and holding back receipts that should be included; and overstating fees and production costs;

- "straight-lining," which improperly allocates the same portion of the licensing fee to every movie or television show in a package without regard to whether it was a hit or failure, which deprives profit participants of a fair allocation of the licensing fees to which they are entitled; and
- improperly delaying, avoiding and misdirecting their audit process.

35. Despite being on notice of these improprieties, Defendants have not paid additional monies due and owing to Plaintiffs. Plaintiffs are informed and believe, and thereon allege, that Defendants willfully and knowingly made misrepresentations to Plaintiffs in order to deprive them of payments they were due under the Series Agreement. Defendants are under a duty to disclose to Plaintiffs the correct amounts due and owing to Plaintiffs based on Defendants' ongoing distribution of *Gilmore Girls* and *Gilmore Girls*: *A Year in the Life*. Defendants intentionally concealed and suppressed the true amounts due and owing to Plaintiffs.

C. Defendants Manipulated Gross Receipts to Deprive Plaintiffs of Payments Due.

36. Defendants also improperly manipulated the MAGR attributable to distribution of *Gilmore Girls* by applying improper deductions, such as the SVOD distribution fees described above, to the MAGR and omitting, deferring, and holding back receipts that should have been included.

37. Defendants supply Plaintiffs with periodic profit participation statements (the "Statements") as part of their regular business practice. The Statements include clearly erroneous and inaccurate information that Defendants knew was false at the time they prepared the Statements.

38. The Statements and the 2014 Audit Report show that Defendants apply – sometimes more than once – improper deductions, which were not agreed to in the Series Agreement, to the MAGR. Examples of these improper deductions include: (1) a deduction for fees associated with SVOD services, like Netflix; (2) overstated indirect overhead expenses and production costs production costs payable to affiliated entities, resulting in artificially reduced

profitability; (3) applying production costs attributable to shows other than *Gilmore Girls* or *Gilmore Girls: A Year in the Life*; (4) electronic sell-through expenses; and (5) video-on-demand expenses. These expenses greatly reduce the MAGR and falsely underrepresent the bottom line number that determines Plaintiffs' profit participation payments, resulting in substantially lower profits paid to Plaintiffs.

39. The Statements also show that Defendants defer and hold back cash receipts that are received and not posted to the Statements in a timely fashion. The delay in posting deprives Plaintiffs of monies due for extended periods of time.

40. Defendants repeatedly submitted Statements to Plaintiffs that do not accurately reflect income generated by and expenses incurred by *Gilmore Girls* and *Gilmore Girls: A Year in the Life*. For example, Defendants understated income and overstated expenses, which showed, that the Subsequent Episodes were incredibly licensed and/or distributed in the same amount as it cost to produce the Subsequent Episodes. Defendants' manipulation of revenues and costs decreased Plaintiffs' participation in these revenues and constitute breaches of the Series Agreement.

D. Defendants Engaged in "Straight-lining" to Avoid Paying Profit Participants.

41. On information and belief, Defendants have engaged in straight-lining by bundling *Gilmore Girls* with unprofitable shows to deprive Plaintiffs of participation profits due.

42. Straight-lining occurs when a television show or film is distributed along with other shows or films for a fee or even for free. Some of the shows and films in a bundle are profitable and some are not. The unprofitable shows yield no payouts to profit participants. By bundling profitable and unprofitable shows and films in this way, a studio may ascribe each title an equal share of the distribution fee and avoid proper allocation of amounts owed to profit participants and the additional fees owed to profit participants of the successful titles. Straight-lining reduces revenue to profitable titles and lowers the MAGR, which in turn results in a lower fee paid based on the negotiated participation percentage.

43. The self-dealing manner in which Defendants allocated revenue to films and television shows included in the bundles resulted in drastic under-allocation of revenues owed to Plaintiffs under the Series Agreement.

E. Defendants' Payment and Audit Process is Designed to Avoid and Defer Making Full Payments to Profit Participants.

44. As noted above, this is the fourth dispute regarding payments due under the Series Agreement since it was executed approximately 18 years ago. Each dispute has required Plaintiffs to expend substantial sums of money and time to obtain the amounts they are owed. Each dispute has resulted in settlements requiring Defendants to pay additional amounts to Plaintiffs. Each of the previous disputes resulted in Plaintiffs' being deprived of monies owed to them for significant periods of time while the disputes were pending. This dispute is no different.

45. The Series Agreement allows a profit participant to conduct an audit of Defendants' books and records. The Series Agreement stipulates that the cost of audits of Defendants' books shall be borne by Plaintiffs, the profit participants. The Series Agreement also necessitates particular strictures to which a profit participant must adhere when engaging in an audit. The restrictions include utilizing specialized auditing firms and lists only three pre-approved auditing firms. Audits are restricted to only one each calendar year, and an audit may not last for longer than 30 days. These are standard provisions, which (on information and belief) are contained in all of Defendants' profit participation agreements. These standard restrictions are adhesive in nature and constitute significant barriers to Plaintiffs' (and other profit participants') ability to maintain a proper system of checks and balances on the amounts they are owed.

46. Additionally, Defendants inappropriately and unnecessarily delay access to audits, which are serviced on a first-in, first-out basis.

47. On or about February 7, 2017, Plaintiffs notified Defendants of their request an audit for amounts in dispute dating back to October 2012.

48. Defendants delayed an entire year – until February 12, 2018 – before providing Plaintiffs with an estimated audit date. At that time, Defendants estimated an audit commencement date of late 2019.

49. Despite their contractual obligations to act in good faith and provide Plaintiffs with reasonable access to books of accounts that accurately reflect the transactions relating to *Gilmore Girls*, Defendants denied Plaintiffs access to information from October 2012 through the date of this complaint, and denied Plaintiffs the right to audit during these periods.

50. Plaintiffs have already been deprived of payments rightfully due for over six years and, given Defendants' timeline, Plaintiffs will suffer lost profits for at least seven years. As a result, Plaintiffs have filed this action to recover amounts Defendants have wrongfully deprived them of since October 2012.

51. Given the prior disputes and audit delays, the parties entered a tolling agreement that preserved Plaintiffs' rights to challenge the issues alleged herein.

FIRST CAUSE OF ACTION

(Breach of Contract Against All Defendants)

52. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

53. By executing the Series Agreement on February 16, 2000, the parties entered into a valid, binding, enforceable contract. The parties incorporated the Modification Agreement and the terms of the settlement agreement from the Third Dispute into the Series Agreement.

54. Plaintiffs fully performed all conditions, covenants, and promises required to be performed under the terms and conditions of the Series Agreement, except for those obligations waived, excused, or prevented by Defendants, its successors in interest, Does 1 through 10, inclusive, and each of them.

55. Defendants have materially breached the Series Agreement by failing to perform their duties under the terms therein (and the terms of the Modification Agreement, to the extent it is incorporated in the Series Agreement). Defendants' failure to perform under the terms of the Termination Agreement include:

- Improperly manipulating gross receipts by adding improper deductions, such as SVOD distribution fees on first run Subsequent Episodes of *Gilmore Girls: A Year in the Life*; omitting deferring, and holding back receipts that should be included; and overstating fees, as described in paragraphs 4, 24, 31-34, 36-40, above;

- "straight-lining," as described in paragraphs 5, 34, and 41-43, above; and
- improperly delaying, avoiding and misdirecting their audit process as described specifically in paragraphs 6, 34, 44-51, above.

56. As a direct and proximate result of these material breaches of the Series Agreement, Plaintiffs have suffered damages in an amount to be proven at trial, but including without limitation the sum Plaintiffs would have received if they had been paid for *Gilmore Girls* and *Gilmore Girls: A Year in the Life* as provided by the Series Agreement.

SECOND CAUSE OF ACTION

(Breach of Fiduciary Duty Against All Defendants)

57. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

58. The relationship between Plaintiffs and Defendants constituted a joint venture as a matter of law because: Plaintiffs and Defendants combined their property, skill, and knowledge in order to carry out a single business undertaking, i.e. *Gilmore Girls*; both Plaintiffs and Defendants have an ownership interest in *Gilmore Girls*; Plaintiffs and Defendants have joint control over *Gilmore Girls*; and Plaintiffs and Defendants agreed to share in the profits and losses of *Gilmore Girls*.

59. By virtue of the joint venture relationship, Defendants owed fiduciary duties to Plaintiffs as a matter of law, including a duty to act with the utmost good faith in the best interests of Plaintiffs.

60. Defendants breached their fiduciary duties by knowingly acting adverse to the interests of Plaintiffs, as set forth above. Defendants also breached their fiduciary duties to Plaintiffs as a result of actions taken by executives employed by Defendants, which were taken solely for personal and not for professional reasons.

61. Plaintiffs are informed and believe and thereon allege that Defendants actively participated in such breaches for the purpose of advancing each of their own interests and financial advantages, including by increasing their reported revenues and profits (and/or decreasing their reported costs) at the expense of Plaintiffs' fair share of profits.

62. As a direct and proximate result of the wrongdoing alleged herein, Plaintiffs have suffered damages as set forth above, in an amount to be determined at trial.

63. By engaging in the misconduct alleged herein, Defendants have acted with malice, oppression and/or fraud, all in willful disregard of Plaintiffs' rights and interests, thus entitling Plaintiffs to an award of punitive or exemplary damages in an amount appropriate to punish or make an example of Defendants, pursuant to Section 3294 of the Civil Code.

THIRD CAUSE OF ACTION

(Breach of the Implied Covenant of Good Faith and Fair Dealing Against All Defendants)

64. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

65. Incorporated into every contract is an implied covenant of good faith and fair dealing, which imposes on each party to the contract an obligation not to take any act or make any omission that would deprive the other party of the benefits and protections of the contract.

66. The Series Agreement contains an implied covenant of good faith and fair dealing prohibiting Defendants from doing anything to deprive Plaintiffs of the benefits and protections therein, specifically from failing to provide accurate and timely earnings reports to Plaintiffs and by failing to act in good faith to maximize payments to Plaintiffs.

67. Defendants breached the implied covenant of good faith and fair dealing in the Series Agreement by willfully and in bad faith failing to abide by the requirement to make accurate Statements and profit participation payments to Plaintiffs for *Gilmore Girls* and *Gilmore Girls: A Year in the Life*. Defendants also failed to maximize the profits due Plaintiffs by self-dealing in its license agreements with affiliated entities and licensing *Gilmore Girls* in packages with less popular projects and not allocating license fees accurately, and licensing films for free but allocating revenues to such projects (i.e., "straight-lining"), which cost Plaintiffs significant revenues. Defendants further breached the implied covenant and acted in bad faith by improperly delaying, avoiding and misdirecting their audit process.

68. By virtue of their conduct, Defendants have deprived Plaintiffs of the benefits of their bargain as set forth in the Series Agreement.

69. As a direct, foreseeable, and proximate result of Defendants' breach of the implied covenant of good faith and fair dealing, Plaintiffs have suffered damages in an amount to be proven at trial.

FOURTH CAUSE OF ACTION

(Fraud Against All Defendants)

70. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

71. Defendants willfully and knowingly made false representations of material fact to Plaintiffs by intentionally providing Plaintiffs with inaccurate accounts of the production and distribution costs associated with *Gilmore Girls* and *Gilmore Girls: A Year in the Life* and the revenues earned by Defendants' distribution of *Gilmore Girls* and *Gilmore Girls: A Year in the Life*. Defendants are under a duty to disclose to Plaintiffs the correct amounts owing to Plaintiffs from the exploitation of *Gilmore Girls* and *Gilmore Girls: A Year in the Life*, and Defendants repeatedly misrepresented, concealed and suppressed the true amounts owing to Plaintiffs.

72. Defendants also made omissions of material facts by failing to inform Plaintiffs that *Gilmore Girls* would be included in packages when licensed, and that Defendants made internal "adjustments" to the income and expenses attributed to *Gilmore Girls* that do not accurately reflect the financial performance of *Gilmore Girls*. Income derived from *Gilmore Girls* was higher than Defendants reported in the Statements and expenses were lower than those reported, and Defendants were under a duty to disclose the correct information to Plaintiffs. Defendants also fraudulently allocated to *Gilmore Girls* a smaller portion of licenses fees charged for the distribution of television shows and films than *Gilmore Girls* deserved. As a result of these actions, Defendants actively endeavored to keep Plaintiffs uninformed of the true amounts owing to them under the Series Agreement.

73. Defendants made these misrepresentations and omissions for years without Plaintiffs' knowledge. Persons employed by Defendants who misrepresented the financial performance of *Gilmore Girls* and expenses attributed to *Gilmore Girls* are not currently known to

Plaintiffs because the entirety of information concerning the methods of accounting for *Gilmore Girls* resides with Defendants.

74. Plaintiffs relied on the accuracy of the information represented in the Statements and other representations made by Defendants. Plaintiffs accepted and relied on Defendants' representations in participation statements based on the parties' long-standing relationship of trust and confidence. This reliance on Defendants' years of misrepresentations caused Plaintiffs to continue their dealings with Defendants to their detriment when they could have ended their relationship with Defendants and endeavored to work with another studio or sue to enforce their rights at an earlier date.

75. Plaintiffs' active reliance on these false representations was reasonable because Defendants possessed all the relevant accounting information and it provided no indication that the dollar amounts it represented as owing to Plaintiffs were inaccurate. The parties are long-time business partners whose joint venture resulted in the production of the successful and memorable television show *Gilmore Girls* and whose relationship can be defined as one of trust and confidence. Defendants violated this trust and Plaintiffs reasonably relied on years of misrepresentations to their detriment.

76. As a direct and proximate result of Defendants' fraudulent conduct, Plaintiffs have been damaged in an amount to be proven at trial, but which amount is in excess of the minimum jurisdictional requirements of this Court.

77. The aforementioned acts were willful, wanton, malicious, oppressive, fraudulent, and were undertaken with the intent to frustrate Plaintiffs' rights. Plaintiffs are therefore entitled to an award of exemplary and punitive damages.

FIFTH CAUSE OF ACTION

(Negligent Misrepresentation Against All Defendants)

78. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

79. Defendants made false representations of material fact to Plaintiffs by providing Plaintiffs with inaccurate accounts of the production and distribution costs associated with

Gilmore Girls and *Gilmore Girls: A Year in the Life* and the revenues earned by Defendants distribution of *Gilmore Girls* and *Gilmore Girls: A Year in the Life*.

80. Defendants also made omissions of material facts by failing to inform Plaintiffs that Defendants made internal "adjustments" to the income and expenses attributed to *Gilmore Girls* that do not accurately reflect the financial performance of *Gilmore Girls* and *Gilmore Girls: A Year in the Life*. Income derived from *Gilmore Girls* was higher than Defendants reported in the Statements and expenses were lower than those reported. Defendants also incorrectly allocated to *Gilmore Girls* a smaller portion of licenses fees charged for the distribution of *Gilmore Girls* than it deserved.

81. Defendants made these misrepresentations and omissions negligently for years without Plaintiffs' knowledge. Plaintiffs relied on the accuracy of the information represented in the Statements, and had Plaintiffs been made aware of the falsity of such representations, they would have severed the entirety of their business relationship with Defendants and sought remedies at law and equity immediately. Mr. Polone is an A-list executive producer who has earned the luxury of choosing the studios with which he does business. Plaintiffs accepted and relied on Defendants' representations in participation statements based on the parties' longstanding relationship of trust and confidence. This reliance on Defendants' years of misrepresentations caused Plaintiffs to continue their dealings with Defendants to their detriment when they could have ended their relationship with Defendants and endeavored to work with another studio or sought remedies at law and equity immediately.

82. Plaintiffs' active reliance on these false representations was reasonable because Defendants possessed all the relevant accounting information and it provided no indication that the dollar amounts it represented as owing to Plaintiffs were inaccurate. The parties are long-time business partners whose joint venture resulted in the production of the successful and memorable television show *Gilmore Girls* and whose relationship was one of trust and confidence. Plaintiffs reasonably relied on years of misrepresentations to their detriment.

83. As a direct and proximate result of Defendants' misrepresentations, Plaintiffs have been damaged in an amount to be proven at trial, but which amount is in excess of the minimum jurisdictional requirements of this Court.

SIXTH CAUSE OF ACTION

(Unfair Business Practices; Violation of Cal. Bus. & Profs. Code §§ 17200 et seq. Against All Defendants)

84. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

85. Polone asserts this claim against all Defendants on behalf of themselves as well as the general public, including other profit participants.

86. Defendants have engaged in at least the following unfair and/or fraudulent conduct constituting unfair competition under California Business and Professions Code Section 17200:

a. Defendants willfully and knowingly made misrepresentations in its accountings to Plaintiffs in order to avoid paying sums owed to Plaintiffs;

b. Defendants wrongfully and unlawfully tied the sale of motion pictures produced by Plaintiffs to other projects and offered them for sale only as part of packages of television shows and films (i.e, "straight-lining"); and

c. Defendants created false Statements that underreported income derived from certain income sources and overreported expenses associated with *Gilmore Girls* and *Gilmore Girls: A Year in the Life*.

87. Plaintiffs are informed and believe and thereon allege that Defendants undertook these acts in order to wrongfully deny Plaintiffs monies and credits owed to them under the terms of the Series Agreement.

88. Plaintiffs are also informed and believe, and on that basis allege, that Defendants are engaged in these unfair and fraudulent business practices with respect to other profit participants besides Plaintiffs.

89. This unfair, fraudulent and self-dealing conduct committed by Defendants has resulted in benefit to Defendants, including without limitation Defendant's retention of monies,

recognition and reputation gain to which Plaintiffs are entitled. Plaintiffs are therefore entitled to the restitution or disgorgement of profits derived from the acts of unfair competition by Defendants, and a temporary restraining order, preliminary and permanent injunction all enjoining Defendants from engaging in further acts of "straight-lining," improperly accounting for monies due to profit participants, and improperly delaying, avoiding and misdirecting their audit process, as well as reasonable costs and attorney's fees. Plaintiffs also pray for a preliminary and permanent injunction preventing Defendants from engaging in the business practices of "straight-lining," fraudulently misreporting income and expenses in their accounting to profit participants, and improperly delaying, avoiding and misdirecting their audit process, including those besides Plaintiffs, and for costs and attorney's fees in pursuit thereof.

SEVENTH CAUSE OF ACTION

(Unlawful Tying Agreement; Violation of Cal. Bus. & Profs.Code §§ 16720 *et seq.* Against All Defendants)

90. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

91. Defendant engaged in unlawful conduct when it linked the sale of *Gilmore Girls* produced by Plaintiffs to the sale of other lesser television shows or films as a necessary prerequisite to the purchase thereof (i.e., "straight-lining").

92. Defendants have significant power in the television and film distribution industry and, as such, have sufficient economic power to coerce the purchase of its packages.

93. Defendants effectuated a substantial amount of sales through its unlawful tying of television show and film packages.

94. As a direct, foreseeable, and proximate cause of Defendants' conduct in tying its products as a prerequisite to their sale, Plaintiffs have suffered damages in an amount to be proven at trial.

95. Defendants' unfair and unlawful conduct as set forth above has caused injury to Plaintiffs, and Plaintiffs therefore are entitled to the recovery of treble damages, as well as reasonable attorneys' fees and costs.

EIGHTH CAUSE OF ACTION

(Accounting Against All Defendants)

96. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

97. Pursuant to the terms of the Series Agreement, Plaintiffs are entitled to an accounting by Defendants, and Defendants are required to permit audits and cooperate with such audits of the accounting books and records of Defendants.

98. Despite demand therefore, Defendants have failed and refused, and continues to fail and refuse, to provide Plaintiffs with proper, accurate, and complete accountings reflecting all revenues derived from Defendants' distribution of *Gilmore Girls* produced by Mr. Polone, and *Gilmore Girls: A Year in the Life* and has further failed and refused, and continues to fail and refuse, to allow Plaintiffs to inspect the books and records of Defendants.

99. Plaintiffs are entitled to a preliminary and permanent injunction requiring Defendants or its successors in interest to provide a complete and accurate accounting of such revenues to date and to further provide complete and timely cooperation with an audit by Plaintiffs or their agents of the accounting records of Defendants with respect thereto.

NINTH CAUSE OF ACTION

(Constructive Trust Against All Defendants)

100. Plaintiffs reallege and incorporate herein by reference each and every allegation contained in the foregoing paragraphs above.

101. Plaintiffs are informed and believe, and on that basis allege, that the monies and/or financial benefits obtained by Defendants as a result of the fraud, misrepresentation and unlawful tying agreements as described herein, were paid to Defendants.

102. Plaintiffs are informed and believe, and on that basis allege, that Defendants knew or reasonably should have known, at the time of the receipt of said funds and/or financial benefits, from Plaintiffs directly or from Defendants as alleged herein, that said funds and/or financial benefits were misappropriated, were obtained as a result of fraud, misrepresentation, and/or illegal tying agreements, and were generally the property of Plaintiffs.

103. Plaintiffs are informed and believe, and on that basis allege, that Defendants at all material times knew or reasonably should have known, that the funds and/or financial benefits received by them were misappropriated assets and the property of Plaintiffs.

104. Plaintiffs are entitled to the proceeds from the acts alleged herein and any and all profits and assets generated thereby that Defendants have derived from said acts.

105. Plaintiffs are informed and believe, and on that basis allege, that Defendants herein own and possesses tangible assets consisting of profits from or monies and/or financial benefits obtained by Defendants' unlawful acts, as alleged herein.

106. Plaintiffs are thus entitled to a constructive trust over all revenues, assets, and profits that Defendants or its successors in interest received as a result of its distribution of *Gilmore Girls* and *Gilmore Girls: A Year in the Life*.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for relief against Defendants as follows:

1. For compensatory and consequential damages in an amount to be proven at trial; including pro-rated costs, with interest at the maximum rate permitted by law;

2. For exemplary and punitive damages;

3. For treble damages;

4. For restitution and disgorgement of profits derived from acts of unfair competition by Defendants;

5. For preliminary and permanent injunctive relief enjoining Defendants from engaging in their fraudulent business practices of (1) inaccurately reporting income and expenses on television shows and films to profit participants, including Plaintiffs; (2) straight-lining; and (3) requiring Defendants and/or their successors in interest to provide a complete and accurate accounting to profit participants, including Plaintiffs; and (4) requiring complete and timely cooperation for an audit by Plaintiffs, their agents, or other profit participants, of the accounting books and records of Defendants.

6. For a declaration that Defendants have breached their duties to Plaintiffs as alleged herein;

7. For a constructive trust over all revenues, assets, and profits that Defendants and/or their successors in interest received as a result of their distribution of *Gilmore Girls* and *Gilmore Girls: A Year in the Life*.

8. For reasonable attorneys' fees and costs; and

9. For any and all other relief found to be just and proper.

DATED: March 13, 2018

BROWNE GEORGE ROSS LLP
Eric M. George
Jeffrey C. Berman

By _____
Jeffrey C. Berman
Attorneys for Plaintiffs Hofflund/Polone and Gavin Polone

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury to the full extent permitted by law.

DATED: March 13, 2018

BROWNE GEORGE ROSS LLP
Eric M. George
Jeffrey C. Berman

By _____
Jeffrey C. Berman
Attorneys for Plaintiffs Hofflund/Polone and Gavin Polone

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

Muhammad Ali Enterprises LLC, Plaintiff, v. Fox Broadcasting Company, Defendant.	Case No. 1:17-cv-7273

COMPLAINT

Plaintiff Muhammad Ali Enterprises LLC, by its attorneys, for its complaint against Fox Broadcasting Company, states as follows:

THE PARTIES

1. Plaintiff Muhammad Ali Enterprises LLC ("MAE") owns the trademark rights, copyrights, right of publicity, and all other intellectual property rights of boxing legend Muhammad Ali.

2. Defendant Fox Broadcasting Company ("Fox") is a major commercial television network that broadcasts its programs throughout the United States.

NATURE OF THE CASE

3. This case arises out of Fox's unauthorized use of Muhammad Ali's identity in a promotional video that Fox broadcast immediately before the start of Fox's broadcast of the 2017 Super Bowl. MAE brings these claims for false endorsement and violation of the right of publicity against Fox for the damages caused and profits unjustly gained by Fox for its unauthorized use of Muhammad Ali's identity.

JURISDICTION

4. Count I of this action arises under the Lanham Act of 1946, as amended, 15 U.S.C. §§ 1051 et seq. This Court has jurisdiction over this claim under 15 U.S.C. §§ 1121 and 28 U.S.C. §§ 1331 and 1338.

5. Count II of this action arises under state statutory law. This Court has jurisdiction over this claim under 28 U.S.C. § 1338(b) in that this claim is joined with a substantial and related claim brought under the trademark laws of the United States (15 U.S.C. §§ 1051 et seq.). This Court also has supplemental jurisdiction over the state law claim under 28 U.S.C. § 1367 because the federal and state claims are based on the same operative facts, and because judicial economy, convenience, and fairness to the parties will result if the Court assumes and exercises jurisdiction over the state law claim.

6. This Court has personal jurisdiction over Fox because it regularly conducts business in this District and caused the promotional video at issue to be disseminated throughout the District.

FACTUAL BACKGROUND

Muhammad Ali: "The Greatest"

7. Muhammad Ali, who died in 2016 at the age of 74, was given the name Cassius Marcellus Clay by his parents, took the name Muhammad Ali when he converted to Islam, and earned the names "The Greatest," "The People's Champion," "The Louisville Lip," and "The King of Boxing" during his lifetime.

8. Ali learned to box as a 12-year-old boy, after his new red and white bicycle, which his father had given him, was stolen. Young Cassius Clay vowed he was "gonna whup whoever stole my bike!" A Louisville policeman, Joe Martin, counseled the boy not to make idle threats and took Cassius under his wing. Martin trained Cassius to box for six months, after

which he won his debut boxing match in a three-round decision.

9. After winning a gold medal in the 1960 Summer Olympics in Rome, Cassius Clay, as he was still known, turned professional later that year, and in 1964 at the age of 22, won the heavyweight boxing title after defeating Sony Liston in an upset. That same year, Ali converted to Islam and was forever known as Muhammad Ali.

10. In 1966, Ali refused to be drafted, citing his objection to the Vietnam War and his religious beliefs. He was arrested, tried, and convicted for draft evasion and stripped of his boxing titles. The Supreme Court overturned his conviction in 1971, and Ali's principled stance against the war as a conscientious objector made him an icon to many in a tumultuous time in modern American history.

11. Despite being sidelined from boxing for four years before his conviction was overturned, Ali went on to earn additional heavyweight titles in 1974 and 1978. *Sports Illustrated* named him the greatest athlete of the 20th century, and the BBC named Ali the Sports Personality of the Century. He is the only boxer to have earned *The Ring* magazine's designation of Fighter of the Year six times.

12. Ali developed a reputation for provocative trash talking, using rhyming and poetry to make his points, anticipating rap and hip-hop music. He recorded two spoken word albums and was twice nominated for a Grammy Award. After his retirement from boxing, Ali dedicated his life to religious and charitable causes. He died on June 3, 2016.

13. Muhammad Ali had, and through his endorsement company MAE, continues to have enormous success as an endorser of carefully selected products and services in which high-quality businesses that wish to profit from an association with Ali contracted with him and now MAE to use aspects of his world-famous identity, including his image and persona, in their

advertising and marketing materials.

14. By carefully controlling the nature and frequency of his product endorsements – rejecting far more requests to use his name and persona than he grants – Ali and MAE have enhanced and maintained the value of his legacy and endorsements.

15. The majority of Ali's and MAE's income was and continues to be derived from MAE's ability to license Muhammad Ali's name and persona to commercial sponsors who wish to capitalize on his fame.

16. Because of the public's widespread knowledge and recognition of Muhammad Ali and admiration for him, goods and services endorsed by and associated with Ali through his endorsement company MAE have come to be well and favorably known and have benefitted greatly from their association with him.

17. Muhammad Ali's name and persona have developed enormous commercial value and secondary meaning in promoting products and services as a result of the public's widespread knowledge and admiration of him.

Fox's Unauthorized Use of Muhammad Ali's Identity

18. Fox broadcast Super Bowl LI in February 2017 to a nationwide audience, estimated to be over 111 million viewers.

19. Fox used Muhammad Ali's name, image, and likeness as the centerpiece of its three-minute promotional video for its broadcast of Super Bowl LI. Fox aired its video immediately before its broadcast of the Super Bowl.

20. The video begins with a narrator who says, "Walk with me. Walk with me as I confront greatness" while the viewer sees the back of a boxer meant to be Ali, wearing a robe that says "The Greatest. The Lip." The viewer sees actual film footage of Ali, as the viewer hears Ali shouting, "I am the Greatest!" The narrator continues, again imploring, "Walk with

me. I can show you what it means to be the greatest."

21. Throughout the video, it refers to and depicts Ali, following him through his boxing career and highlighting his controversies and personal achievements, including his principled stance as a conscientious objector and his lighting the torch at the 1996 Summer Olympics in Atlanta. The video informs or reminds the viewer of the characteristics and accomplishments that made Ali "The Greatest," repeatedly defining "greatness" with examples Ali set in his life.

22. But Fox's promotional video, entitled "The Greatest," is far more than a tribute to Muhammad Ali, who had died eight months before Super Bowl LI and whose fame and reputation were in the public consciousness when the video was shown. In the second half of the video, while continuing the theme of greatness, the focus shifts to imagery of NFL legends, including Joe Montana, Jerry Rice, Troy Aikman, Emmitt Smith, Joe Namath, John Elway, Tom Brady, Vince Lombardi, and Peyton Manning.

23. The video uses Ali to define greatness and ultimately to compare the NFL legends to Ali and thus to define them and the Super Bowl as "greatness" too. The narrator tells the viewer that "in the Super Bowl many have marched towards this same confrontation with greatness." Juxtaposing images of Ali walking down a tunnel with those of Super Bowl greats walking in a tunnel on their way to the playing field, the narrator invites the viewer to "walk with me to that light at the end of the tunnel." He concludes that "it's the only way to prove you're worthy of being called 'The Greatest.'"

24. At the conclusion of the video, the screen displays the logo of Super Bowl LI and concludes with another screen that includes Muhammad Ali's name and the years of his birth and death.

25. Fox never requested or received MAE's permission to use Ali's identity or to imply his endorsement in connection with the services offered by Fox, including its broadcast of the Super Bowl.

26. Fox's promotional video uses Ali's identity to promote Fox and its broadcast services.

27. Fox's promotional video is likely to confuse consumers as to Ali's and MAE's sponsorship or approval of those services.

28. Fox could have sold the three minutes it used for its promotional video to other advertisers for $30 million.

29. MAE has been damaged by Fox, whose unauthorized promotional video infringes Ali's right of publicity, assigned to MAE, and falsely conveys Ali's and MAE's endorsement of Fox's services, leading consumers to wrongly conclude that Ali or MAE endorses those services.

COUNT I

(MAE'S CLAIM FOR VIOLATION OF SECTION 43(a) OF THE LANHAM ACT – FALSE ENDORSEMENT)

30. MAE realleges and incorporates by reference paragraphs 1 through 29 of this Complaint.

31. Fox's unauthorized use of Ali's identity, including his image and persona, in its promotional video was a false or misleading representation of fact that falsely implies Ali's or MAE's endorsement of Fox's services.

32. Fox's unauthorized use of Ali's identity

(a) is likely to cause confusion, mistake, or deception as to the affiliation, connection, or association of Fox with Ali or MAE, or as to the origin, sponsorship, or approval of Fox's services or commercial activities by Ali or MAE in violation of Section 43(a) of the

Lanham Act, 15 U.S.C. § 1125(a)(1)(A); or

(b) misrepresents the nature, characteristics, or qualities of Fox's services or commercial activities in violation of Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a)(1)(B).

33. MAE has been damaged by these acts. MAE has no adequate remedy at law.

34. This case is an exceptional case pursuant to 15 U.S.C. § 1117.

WHEREFORE, MAE requests that relief be granted in its favor and against Fox for (a) damages sustained by MAE, including Fox's profits, in an amount greater than $30,000,000, such damages to be trebled pursuant to 15 U.S.C. § 1117, (b) attorneys' fees and costs, (c) a permanent injunction requiring Fox to refrain from any use of Ali's identity without prior authorization from MAE, (d) an order requiring Fox to delete or cause to be deleted all copies of the promotional video from any website or other location, and (e) such other and further relief as the Court deems just and proper.

COUNT II

(MAE'S CLAIM FOR VIOLATION OF THE ILLINOIS RIGHT OF PUBLICTY ACT)

35. MAE realleges and incorporates by reference paragraphs 1 through 29 of this Complaint.

36. Fox's unauthorized use of Ali's identity for commercial purposes is a violation the Illinois Right of Publicity Act, 765 ILCS 1075/1-60.

37. Fox's use of Ali's identity was unauthorized because Fox did not obtain Ali's or MAE's written consent to use Ali's identity in connection with the promotional video. In fact, Fox did not even request Ali's or MAE's consent.

38. Fox's use of Ali's identity was willful because Fox used Ali's identity

intentionally and with knowledge that its use was not authorized.

39. MAE has been damaged by Fox's unauthorized use of Ali's identity.

WHEREFORE, MAE requests that relief be granted in its favor and against Fox for (a) damages sustained by MAE, including Fox's profits, in an amount greater than $30,000,000, (b) punitive damages, (c) attorneys' fees and costs, (d) a permanent injunction requiring Fox to refrain from any use of Ali's identity without prior authorization from MAE, (e) an order requiring Fox to delete or cause to be deleted all copies of the promotional video from any website or other location, and (f) such other and further relief as the Court deems just and proper.

JURY DEMAND

MAE hereby demands a trial by jury.

Dated: October 10, 2017

/s/ Frederick J. Sperling

Frederick J. Sperling
Clay A. Tillack
David C. Giles
Ann H. MacDonald
Brooke Clason Smith

SCHIFF HARDIN LLP
233 South Wacker Drive
Suite 7100
Chicago, IL 60606
(312) 258-5500

Attorneys for Plaintiff
Muhammad Ali Enterprises LLC

Privacy and the Internet of Things (IoT)

Leonie Huang, Esq.
Holland & Knight (Moderator)

Mark Melodia, Esq.
Partner, Holland & Knight

Jessica Lee, Esq.
Partner, Loeb & Loeb

Anthony Ford, Esq.
Senior Data Privacy Counsel, Medidata Solutions, Inc.

Manas Mohapatra, Esq.
Chief Privacy Officer at Viacom

The Internet of Things ("IoT") – Background Information

Compiled by Leonie Huang, Holland & Knight

I. What is the IoT?

A. Where did the term come from?: Kevin Ashton is often credited with coining the term in 1999, while working as a brand manager at Proctor & Gamble and working on early RFID technology. (Kevin Ashton is a cofounder of the Auto-ID Center at Massachusetts Institute of Technology, a precursor to the Auto-ID Lab at MIT— which is part of an independent network of seven academic research labs conducting research and development of new technologies with a goal of creating new consumer benefits and revolutionizing global commerce.)

1. Sources:

a. Internet of things (IoT) History, Postscapes (Aug. 20, 2018), https://www.postscapes.com/internet-of-things-history/ ("1999 - A big year for the IoT and MIT. The Internet of Things term is coined by Kevin Ashton executive director of the Auto-ID Center").

b. Kevin Ashton, "*That "Internet of Things" Thing*, RFID Journal (June 22, 2009), available at https://www.rfidjournal.com/articles/view?4986 ("I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999.")

c. Arik Gabbai, *Kevin Ashton Describes "the Internet of Things"*, Smithsonian Magazine (January 2015), available at https://www.smithsonianmag.com/innovation/kevin-ashton-describes-the-internet-of-things-180953749/#i6DUCkEK2jE8yH6V.99

d. Kevin Maney and Alison Maney, *Kevin Ashton, Father of the Internet of Things & Network Trailblazer*, Cisco - The Network (Dec. 8, 2014), available at https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1558161 ("It all started with lipstick. A particularly popular color of Oil of Olay lipstick that Kevin Ashton had been pushing as a brand manager at Procter & Gamble was perpetually out of stock. He decided to find out why, and found holes in data about the supply chain that eventually led him to drive the early deployment of RFID chips on inventory. Asked by the Massachusetts Institute of Technology to start a group -- the Auto-ID Center -- that would research RFID technology, he found a way to talk about RFID to a less-than-computer-savvy crowd – by coining the phrase the Internet of Things or IoT.").

i. RFID: "Radio Frequency IDentification is a technology that allows almost any object to be wirelessly identified using data transmitted via radio waves." Suzanne Smiley, *What is RFID*, RFID Insider (Feb. 21, 2017), available at https://blog.atlasrfidstore.com/what-is-rfid?utm_source=Quick-Start&utm_medium=Link&utm_campaign=Content&utm_content=What-is-RFID

B. How do people define IoT?: There are many definitions and descriptions. Commenters say there is no generally or universally agreed definition. Here are some recent definitions excerpted from the source documents noted at the end of each excerpt:

1. "Internet of Things" (IoT) refers to networks of objects that communicate with other objects and with computers through the Internet. The objects that are not themselves computers but have embedded components that connect to the Internet.

a. Things" may include virtually any object for which remote communication, data collection, or control might be useful, such as smart meters, fitness trackers, smart clothing, vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment, or building systems.

i. In other words, the IoT potentially includes huge numbers and kinds of interconnected objects.

b. Two features makes objects part of the IoT—a unique identifier and Internet connectivity.

i. Such "smart" objects each have a unique Internet Protocol (IP) address to identify the object sending and receiving information.

ii. Smart objects can form systems that communicate among themselves, usually in concert with computers, allowing automated and remote control of many independent processes and potentially transforming them into integrated systems.

c. Source: Eric A. Fischer, *The Internet of Things: Frequently Asked Questions*, Congressional Research Service Report (October 13, 2015), available at https://crsreports.congress.gov/product/pdf/R/R44227

2. Although there is no single, universal definition for IoT, the term generally refers to a network of ordinary objects that are embedded with Internet-connected electronics, sensors, or software that can capture, exchange, and receive data.

a. These “things” include items sold to and used by consumers, as well as broader cloud-enabled machine-to-machine communications that enable businesses and organizations to track energy use, functionality, or efficiency.

b. IoT technology enables the creation, transmission, communication, and analysis of data generated by embedded sensors.

c. See Table ES-1 at page 2 for an overview of technologies facilitating IoT information exchange.

d. Source: Federal Transit Administration, Report to Congress on Internet of Things, FTA Report No. 0099 (Feb. 2017), available at https://www.transit.dot.gov/sites/fta.dot.gov/files/docs/research-innovation/60436/ftareportno0099.pdf

II. When did the IoT really take off?

A. According to Cisco Internet Business Solutions Group, there came a point in time (sometime between 2008 and 2009) when more things than people were connected to the internet, and the IoT was “born.”

Source: Dave Evans, *The Internet of Things, How the Next Evolution of the Internet Is Changing Everything*, Cisco White Paper 3 (April 2011), available at https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

B. More recently, with 5G wireless capability people are again talking about a takeoff of IoT.

Examples:

- Hatem Zeine, What The Future Of IoT And 5G May Look Like, Forbes.com (Nov. 1, 2018), available at https://www.forbes.com/sites/forbestechcouncil/2018/11/01/what-the-future-of-iot-and-5g-may-look-like/#48341af0629b

- Corrine Reichert, *CES 2019: Sprint pairs Curiosity IoT with 5G to power smart cities, autonomous vehicles*, ZDNet (Jan. 9, 2019), available at https://www.zdnet.com/article/ces-2019-sprint-pairs-curiosity-iot-with-5g-to-power-smart-cities-autonomous-vehicles/

III. How many things or devices are we talking about now?

A. Estimates vary widely, for example, ranging from 8.4 billion to 18 billion connected things in 2017 and projections of around 20 to 50 billion by 2020.

1. Sources:

a. Cisco: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc529314172

b. Ericsson: https://www.ericsson.com/en/mobility-report/internet-of-things-forecast

c. Gartner: https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016

IV. IoT in the News – For some recent headlines detailing public concern with privacy and security issues related to the IoT see these examples:

- Laura Hautala, *Blackberry Wants to Make the Internet of Things Safe for You*, CNet (Jan. 6, 2019), available at https://www.cnet.com/news/blackberry-wants-to-make-the-internet-of-things-safe-for-you/

- Jennifer Valentino-Devries, Natasha Singer, Michael H. Keller and Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. Times (Dec. 10, 2018), available at https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

- Farhad Manjoo, *A Future Where Everything Becomes a Computer Is as Creepy as You Feared*, N.Y. Times (Oct. 10, 2018), available at https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html

- Derek Hawkins, *The Cybersecurity 202: California's New Internet of Things Law Only Protects Against a Small Portion of Cyberthreats*, Washington Post (Oct. 8, 2018) available at https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/10/08/the-cybersecurity-202-california-s-new-internet-of-things-law-only-protects-against-a-small-portion-of-cyberthreats/5bba75781b326b7c8a8d1885/?utm_term=.5c55aec4735e

- Lily Hay Newman, *The Sensors that Power Smart Cities are Aa Hacker's Dream*, Wired (Aug. 9, 2018), available at https://www.wired.com/story/sensor-hubs-smart-cities-vulnerabilities-hacks/

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

The people of the State of California do enact as follows:

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. SECURITY OF CONNECTED DEVICES

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

(2) Appropriate to the information it may collect, contain, or transmit.

(3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:

(1) The preprogrammed password is unique to each device manufactured.

(2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

1798.91.05. For the purposes of this title, the following terms have the following meanings:

(a) "Authentication" means a method of verifying the authority of a user, process, or device to access resources in an information system.

(b) "Connected device" means any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address.

(c) "Manufacturer" means the person who manufactures, or contracts with another person to manufacture on the person's behalf, connected devices that are sold or offered for sale in California. For the purposes of this subdivision, a contract with another person to manufacture on the person's behalf does not include a contract only to purchase a connected device, or only to purchase and brand a connected device.

(d) "Security feature" means a feature of a device designed to provide security for that device.

(e) "Unauthorized access, destruction, use, modification, or disclosure" means access, destruction, use, modification, or disclosure that is not authorized by the consumer.

1798.91.06. (a) This title shall not be construed to impose any duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications that a user chooses to add to a connected device.

(b) This title shall not be construed to impose any duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications, to review or enforce compliance with this title.

(c) This title shall not be construed to impose any duty upon the manufacturer of a connected device to prevent a user from having full control over a connected device, including the ability to modify the software or firmware running on the device at the user's discretion.

(d) This title shall not apply to any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority.

(e) This title shall not be construed to provide a basis for a private right of action. The Attorney General, a city attorney, a county counsel, or a district attorney shall have the exclusive authority to enforce this title.

(f) The duties and obligations imposed by this title are cumulative with any other duties or obligations imposed under other law, and shall not be construed to relieve any party from any duties or obligations imposed under other law.

(g) This title shall not be construed to limit the authority of a law enforcement agency to obtain connected device information from a manufacturer as authorized by law or pursuant to an order of a court of competent jurisdiction.

(h) A covered entity, provider of health care, business associate, health care service plan, contractor, employer, or any other person subject to the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) (Public Law 104-191) or the Confidentiality of Medical Information Act (Part 2.6 (commencing with Section 56) of Division 1) shall not be subject to this title with respect to any activity regulated by those acts.

(i) This title shall become operative on January 1, 2020.

SEC. 2. This act shall become operative only if Assembly Bill 1906 of the 2017–18 Regular Session is also enacted and becomes effective.

O

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

BRIAN FLYNN, GEORGE BROWN, KELLY BROWN, and MICHAEL KEITH, ***on behalf of themselves and all others similarly situated,***	)	
Plaintiffs,	)	
vs.	)	**Case No. 15-cv-855-MJR-DGW**
FCA US LLC, and HARMAN INTERNATIONAL INDUSTRIES, INC.,	)	
Defendants.	)	

MEMORANDUM & ORDER

REAGAN, Chief Judge:

Before the Court is a motion to dismiss for lack of personal jurisdiction (Doc. 407) filed by Defendant FCA US LLC on August 22, 2018. Defendant Harman International Industries, Inc. moved to join in the motion on August 24, 2018 (Doc. 408). Plaintiffs responded to the motion to dismiss on September 12, 2018 (Doc. 409), and FCA filed a reply on September 14, 2018. For good cause shown, the motion for joinder (Doc. 408) is **GRANTED**, and the Court considers the arguments in the motion to dismiss with respect to both Defendants.

BACKGROUND

On August 4, 2015, Plaintiffs Brian Flynn, Kelly and George Brown, and Michael Keith filed suit, on behalf of themselves and all others similarly situated, alleging a number of claims related to a design flaw in the uConnect system, which was manufactured by Harman and installed in certain 2013-2015 Chrysler vehicles. The

putative class action sought to certify both a nationwide class and state-based classes, including classes of Michigan consumers and of Missouri consumers. In September 2015, Defendants filed motions to dismiss for failure to state a claim and for lack of standing pursuant to Federal Rules of Civil Procedure 12(b)(6) and Rule 12(b)(1). (Docs. 23, 28). The motions were rendered moot by Plaintiffs' first amended complaint (Doc. 49), but new motions directed at that complaint were filed in February 2016. (Docs. 68, 71). The Court granted the motions in part and denied them in part in September 2016 (Doc. 115), withholding ruling on any arguments brought against the Browns' claims, as they were ordered to arbitrate certain warranty claims.

The Browns decided not to arbitrate, and their warranty claims were dismissed for failure to prosecute. (Doc. 149). Defendants then moved to dismiss the Browns' remaining claims, renewing challenges under Rules 12(b)(1) and 12(b)(6). (Docs. 152, 154, 158). The motions were granted in part and denied in part on August 21, 2017. (Doc. 236). The Court directed Plaintiffs to file a second amended complaint, which Defendants moved to dismiss. (Docs. 249, 254).

In October 2017 and January 2018, Defendants filed seven motions for summary judgment (Docs. 256, 257, 264, 267, 346, 348, 350). Both Harman and FCA filed lengthy oppositions to Plaintiffs' motion to certify class (Docs. 318, 321) and argued against class certification during a January 11, 2018 hearing on Plaintiffs' motion. At the hearing, Defendants also renewed their standing challenge. Following briefing on the renewed challenge, the Court found that Plaintiffs have standing to pursue their claims. Defendants moved the Court to certify the order denying their standing challenge for

interlocutory appeal. The request was granted, and Defendants filed a petition for leave to appeal with the Seventh Circuit Court of Appeals. The Seventh Circuit denied the petition on May 4, 2018. On July 5, 2018, the Court granted in part and denied in part the seven motions for summary judgment and Plaintiffs' motion to certify class. (Doc. 399). Three classes were certified: an Illinois class, a Michigan class, and a Missouri class.

At no point prior to class certification did Defendants challenge, or suggest that they might challenge, the exercise of personal jurisdiction over them. Instead, they raised the issue for the first time in the petition for leave to appeal the class certification order filed with the Seventh Circuit Court of Appeals in July 2018. The Seventh Circuit denied the petition for leave to appeal the class certification order, and Defendants now raise their objection to personal jurisdiction before this Court. For the reasons delineated below, the Court **FINDS** that Defendants waived any objection to personal jurisdiction, and the motion to dismiss for lack of jurisdiction is **DENIED**.

ANALYSIS

A defense based on personal jurisdiction "may be waived if a defendant gives a plaintiff a reasonable expectation that he will defend the suit on the merits or where he causes the court to go to some effort that would be wasted if personal jurisdiction is subsequently found lacking." ***Hedeen Intern., LLC v. Zing Toys, Inc.*, 811 F.3d 904, 906 (7th Cir. 2016)**. Here, the parties have litigated this case fervently for more than three years, and Defendants seemingly acknowledge that the defense is waived as to the named Missouri and Michigan class representatives, Kelly and George Brown and

Michael Keith, by arguing their motion as to the unnamed class members only.. ***See Continental Bank, N.A. v. Meyer*, 10 F.3d 1293, 1296-97 (7th Cir. 1993)(finding personal jurisdiction defense waived where defendants fully participated in litigation for over two and a half years)**. Defendants gave Plaintiffs a reasonable expectation that they would defend this action on the merits by failing to object to personal jurisdiction until after the class certification stage. They also caused the Court to go to some effort that would be wasted if personal jurisdiction now is found to be lacking by pursuing several rounds of motions to dismiss and standing challenges in addition to significant briefing related to summary judgment and class certification before raising the objection.

Defendants attempt to skirt past the waiver issue with an argument that unnamed class members were not parties to the litigation prior to the order certifying classes in this case, suggesting that they could not have challenged personal jurisdiction any earlier than they did. As a preliminary note, the party-status of unnamed class members is not as clear cut as Defendants state it is. ***See e.g., Smith v. Bayer Corp.*, 564 U.S. 299, 313 (2011)(noting that unnamed members of a proposed but uncertified class are not parties when considering preclusion and relitigation exception to Anti-Injunction Act); *Pearson v. Target Corp.*, 893 F.3d 980, 984 (7th Cir. 2018)(acknowledging that "party" does not indicate an absolute characteristic, as absent class members may be parties for some, but not all, purposes)**. When it comes to the question of whether Defendants waived their objection to the exercise of personal jurisdiction with respect to the certified Michigan and Missouri classes, the issue of party-status and the recentness of the addition of unnamed class members to this action

is not determinative. Instead, the question of waiver is weighed against the entire course of this litigation, not just with respect to post-certification events.

Defendants' argument that they had to await a ruling on class certification before raising a challenge to personal jurisdiction relies on cases considering the issue at or before the class certification stage. In ***Biffar v. Pinnacle Foods***, Judge Herndon denied a motion to dismiss for lack of personal jurisdiction over non-Illinois putative class members as premature, noting that the issues should be addressed "at the class certification stage." ***Biffar v. Pinnacle Foods*, 2016 WL 7429130, *6 (S.D. Ill. 2016)(Herndon, J.)**. Defendants draw from that comment that the issue cannot be raised until after a ruling on class certification, which is plainly different than the language in the order. Defendants also cite to class certification order in ***Practice Mgmt. Support Servs., Inc. v. Cirque du Soleil*, 301 F.Supp.3d 840, 861-64 (N.D. Ill. 2018)(Durkin, J.)**, which considered the issue of personal jurisdiction simultaneously with the issue of class certification. Unlike this case, the objection to personal jurisdiction was raised and briefed prior to the ruling on class certification. Defendants cite no cases directly in support of their contention that they had to wait until after class certification to raise personal jurisdiction challenges, and the undersigned finds that they now raise their objection too late.

Litigation of this action has progressed past the class certification stage without any hint of a challenge to personal jurisdiction prior to certification of classes with out-of-state plaintiffs, and the Court is not persuaded by Defendants' suggestion that their delay in raising the issue does not waive their ability to raise the challenge post-

certification. By proceeding through several motions to dismiss, seven motions for summary judgment, and a vigorous defense to class certification without mention of personal jurisdiction, Defendants gave Plaintiffs a reasonable impression that they would defend this suit on the merits. They have fully participated in this action for over three years and have caused the Court to expend more than "some effort" that would be wasted by a finding at this stage that personal jurisdiction is lacking. Accordingly, the Court **FINDS** that Defendants waived any objection to the exercise of personal jurisdiction as to all out-of-state plaintiffs, including the unnamed class members.

CONCLUSION

For the above-stated reasons, Defendant Harman International Industries, Inc.'s motion for joinder (Doc. 408) is **GRANTED** and Defendants' motion to dismiss for lack of jurisdiction (Doc. 407) is **DENIED**.

On July 23, 2018, the Court exercised its discretionary powers and stayed this action in its entirety. The Court hereby **LIFTS the STAY** and sets this case for trial at 9:00 a.m. on Monday, March 11, 2019. A final pretrial conference is set for 10:00 a.m. on Thursday, March 7, 2019.

The parties shall confer regarding class notice and shall file a status report (not to exceed 6 pages) with their joint proposal or competing proposals for notice on or before October 19, 2018.

IT IS SO ORDERED.

DATED: October 9, 2018

s/ Michael J. Reagan
MICHAEL J. REAGAN
United States District Judge

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET AND TECHNOLOGY

In the Matter of

Assurance No. 17-056

Investigation by ERIC T. SCHNEIDERMAN, Attorney General of the State of New York, of

SAFETECH PRODUCTS, LLC, and RYAN HYDE, as an individual,

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("NYAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") §§ 349 and 350 into the security of Safetech Products LLC, and its owner Ryan Hyde ("Respondents"), Bluetooth-enabled locks. This Assurance of Discontinuance ("Assurance") contains the findings of the NYAG's investigation and the relief agreed to by NYAG and Respondents.

FINDINGS OF NYAG

1. Safetech Products, LLC ("Safetech" is a limited liability corporation with a principal place of business at 1601 North State Street, Lehi, Utah. It is owned by Ryan Hyde.

2. Safetech sells Bluetooth-enabled locks to customers through its website https://www.thequicklock.com/ with the promise "Privacy When You Want It, Security When You Need It." With Bluetooth-enabled locks, the user may control the locks with an application ("app") installed on a smartphone.

3. Bluetooth is a wireless technology standard for exchanging data over short distances of up to 300 feet. It uses short-wavelength UHF radio waves in the ISM band from 2.4

to 2.485 GHz. To operate the Bluetooth-enabled lock, the smartphone and the lock must have their Bluetooth antennas turned on at the same frequency band and broadcast their identifiers to each other. A default password is used to secure the connection and exchange data.

4. In August 2016, independent security researchers reported that Respondents' Bluetooth-enabled locks transmitted passwords between the locks and the user's smartphone in plain text and without encryption. The researchers reported that a wrong-doer could intercept the passwords and proceed to unlock the locks. The researchers also reported that the locks contained weak default passwords that were not secure and could be guessed or discovered through brute force attacks (i.e., automated software used to generate a large number of consecutive guesses).

5. In October 2016, the NYAG contacted Respondents about the findings of the researchers and the security of the locks. Just prior to being contacted by the NYAG, Respondents voluntarily placed the following warning on the https://www.thequicklock.com/ website:

> SECURITY WARNING...Bluetooth keys for the hardware are passed "unencrypted" on all current products.
>
> We also strongly recommend the default password be changed at initial setup. Please read "Security Risks Explained."

Upon clicking the "Security Risks Explained" hyperlink, the user is taken to a webpage that explains the risks identified above.

6. Respondents' locks limited the Bluetooth range to approximately 50 feet. Thus, a wrongdoer would need to be in close proximity to the lock to intercept the Bluetooth passwords. Additionally, the locks shutdown for 2 minutes with two failed password attempts. Thus, a brute force attack would be limited by the locks 2-minute lock-out feature.

7. By violating express and implied representations of reasonable data security, Respondents violated New York Executive Law § 63(12) and New York General Business Law §§ 349 and 350.

PROSPECTIVE RELIEF

WHEREAS, Respondents admit NYAG Findings (1)-(6) above;

WHEREAS, NYAG is willing to accept the terms of this Assurance pursuant to Executive Law § 63(15) and to discontinue its investigation into Respondents' representations concerning the security of its Bluetooth-enabled locks; and

WHEREAS, the parties each believe that the obligations imposed by this Assurance are prudent and appropriate;

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the parties, that:

8. This Assurance shall apply to Respondent Safetech Products LLC, and any officers, directors, servants, agents, employees, assignees, and any individual, subsidiary, division, or other entity through which the company may now or hereafter act, as well as any successors-in-interest, and Ryan Hyde, as an individual.

9. Respondents shall comply with Executive Law § 63(12), and GBL §§ 349 and 350, and shall not misrepresent, expressly or by implication, the security of its locks, or the security, confidentiality, or integrity of any data these devices transmit via Bluetooth or other radio frequencies.

10. Respondents shall encrypt all passwords, electronic keys or other credentials ("Security Information") in their locks and other Bluetooth-enabled devices that Respondents market or sell to individual consumers and the general public. Respondents' Bluetooth-enabled

devices shall prompt users to change the default password upon the customer's initial setup of wireless communication.

11. Within 30 days of the execution of this Assurance, Respondents shall establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing devices that use Security Information, and (2) protect the privacy, security, confidentiality, and integrity of Security Information. Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards appropriate to company's size and complexity, the nature and scope of the company's activities, and the sensitivity of the device's function or the information it collects, transmits or processes, including:

a. The designation of an employee or employees to coordinate and be accountable for the security program;

b. The identification of material internal and external risks to (1) the security of the devices that could result in unauthorized access to or unauthorized modification of the device and (2) the privacy, security, confidentiality, and integrity of Security Information;

c. The risk assessments required by subpart b must include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing; (4) review, assessment, and response to third party security vulnerability

reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

d. The design and implementation of reasonable safeguards to control the risks identified through risk assessment;

e. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures including reasonable and appropriate security testing techniques such as vulnerability and penetration testing, security architecture reviews and code reviews;

f. The development and use of reasonable steps to select and retain service providers (if any are hired) capable of maintaining security practices consistent with this Assurance, and requiring service providers by contract to implement and maintain appropriate safeguards consistent with this Assurance; and

g. The evaluation and adjustment of Respondents' security program in light of the results of the testing and monitoring required by subpart e, any material changes to Respondents' operations or business arrangements, or any other circumstances that Respondents' knows or has reason to know may have a material impact on the effectiveness of the security program.

12. Respondents shall, within 10 business days of receiving a written request from NYAG, make available for NYAG review a copy of Respondents' written policies and procedures adopted pursuant to this Assurance or otherwise.

Miscellaneous

13. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondents and its counsel and NYAG's own factual

investigation as set forth in Findings (1)-(6) above. To the extent that any of Respondents' representations are later found to be inaccurate or misleading, this Assurance is voidable by the NYAG in its sole discretion.

14. If the Assurance is voided or breached, Respondents agree that any statute of limitations or other time-related defenses applicable to the subject of the Assurance and any claims arising from or relating thereto are tolled from and after the date of this Assurance. In the event the Assurance is voided or breached, Respondents expressly agree and acknowledge that this Assurance shall in no way bar or otherwise preclude NYAG from commencing, conducting or prosecuting any investigation, action or proceeding, however denominated, related to the Assurance, against the Respondents, or from using in any way any statements, documents or other materials produced or provided by Respondents prior to or after the date of this Assurance.

15. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondents in agreeing to this Assurance.

16. Respondents represent and warrant, through the signatures below, that the terms and conditions of this Assurance are duly approved, and execution of this Assurance is duly authorized. Respondents shall not take any action or make any statement denying, directly or indirectly, the propriety of this Assurance or expressing the view that this Assurance is without factual basis. Nothing in this paragraph affects Respondents' (i) testimonial obligations or (ii) right to take legal or factual positions in defense of litigation or other legal proceedings to which NYAG is not a party. This Assurance may not be used and is not intended for use by any third party in any other proceeding.

17. This Assurance may not be amended except by an instrument in writing signed on

behalf of all the parties to this Assurance.

18. This Assurance shall be binding on and inure to the benefit of the parties to this Assurance and their respective successors and assigns, provided that no party, other than NYAG, may assign, delegate, or otherwise transfer any of his rights or obligations under this Assurance without the prior written consent of NYAG.

19. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the NYAG such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

20. To the extent not already provided under this Assurance, Respondents shall, upon request by NYAG, provide documentation and information necessary for NYAG to verify compliance with this Assurance.

21. All notices, reports, requests, and other communications to any party pursuant to this Assurance shall be in writing and shall be directed as follows:

If to Respondents:

SafeTech Products, LLC
TheQuickLock LLC
1601 North State Street]
Lehi, Utah 84043

If to the NYAG, to:

Attorney General of the State of New York
120 Broadway
New York, New York 10271
Attention: Chief, Bureau of Internet and Technology

22. Acceptance of this Assurance by NYAG shall not be deemed approval by NYAG of any of the practices or procedures referenced herein, and Respondents shall make no

representation to the contrary.

23. Pursuant to Executive Law § 63(15), evidence of a violation of this Assurance shall constitute *prima facie* proof of violation of the applicable law in any action or proceeding thereafter commenced by NYAG.

24. If a court of competent jurisdiction determines that Respondents have breached this Assurance, Respondents shall pay to NYAG the cost, if any, of such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

25. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. The NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding.

26. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

27. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

28. This Assurance may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

ERIC T. SCHNEIDERMAN
NEW YORK ATTORNEY GENERAL
BUREAU OF INTERNET AND TECHNOLOGY

By: Clark Russell
Deputy Bureau Chief

5/9/17
Date

SAFETECH PRODUCTS LLC AND RYAN HYDE

By:

May 3, 2017
Date

New York Attorney General's Office
120 Broadway
New York, NY 10271-0332
Phone: (212) 416-8433
Fax: (212) 416-8369

Privacy and the Internet of Things (IoT)

NYSBA IP Section | January 15, 2019 Annual Meeting

***Mark S. Melodia**, Partner, NY | **Mark H. Francis**, Partner, NY*

1. UNDERSTANDING THE RISKS

a. Data privacy risks typically stem from two key issues:

   i. *Data misuse* such as the unauthorized collection and use an individual's personal information; and

   ii. *Data breach* that compromises an individual's personal information due to insufficient security measures.

b. "Internet of Things" ("IoT") devices present a bigger challenge than traditional systems such as computers for a number of reasons, for example:

   i. Poor software patching practices by manufacturers and users result in IoT vulnerabilities being common and easily exploited;

   ii. Manufacturers may not provide long-term support for IoT devices (*e.g.*, beyond 1-3 years) while they may be in use for much longer periods;

   iii. Many IoT devices incorporate open source software that is not properly understood or secured when adopted by manufacturers (*e.g.*, Linux O/S); and

   iv. Manufacturers compete on price for low-cost IoT devices and security is not a significant consideration in product development.

c. IoT devices therefore present a number of heightened security risks, such as:

   i. Enabling unauthorized access and misuse of users' sensitive personal information maintained or accessible by the IoT device;

   ii. Facilitating attacks on other systems, such as (1) using a compromised IoT device to move laterally to other systems on the network, or (2) using thousands of compromised IoT devices and to facilitate botnet attacks; and

   iii. Creating safety risks and potentially physical harm, such as damaging medical devices (insulin pumps, pacemakers), or taking over vehicle controls.

d. IoT devices also collect more sensitive personal information that traditional computers in many respects—for example, they may have access to precise geolocation data, detailed health information (e.g., fitness trackers) and highly-personal audio and video feeds.

2. REGULATORY GUIDANCE

a. U.S. Department of Homeland Security ("DHS") issued the *Strategic Principles For Securing The Internet Of Things (IoT)* on November 15, 2016,[1] promoting six key practices:

   i. Incorporate security at the design phase;

   ii. Advance security updates and vulnerability management;

   iii. Build on proven security practices;

   iv. Prioritize security measures according to potential impact;

   v. Promote transparency across IoT; and

   vi. Connect carefully and deliberately.

b. Federal Trade Commission ("FTC") Staff Report *internet of things: Privacy & Security in a Connected World* released in January 2015[2] focused on three areas: data security, data minimization, and consumer notice and choice.

c. Also in January 2015, the FTC also released a short summary on IoT Security entitled *Careful Connections: Building Security in the Internet of Things*,[3] promoting adoption of many security concepts for IoT including a culture of security, security by design, defense-in-depth, risk-based approaches and avoidance of default passwords.

---

[1] https://www.dhs.gov/securingtheIoT.

[2] https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[3] https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things.

d. The National Institute of Standards and Technology ("NIST") has been a leading influencer in cybersecurity standards and best practices, most notably the *NIST Cybersecurity Framework*[4]

e. In November 2018, NIST published an *Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT)*[5] to inform and support policymakers, businesses, and other interested participants on development and use of cybersecurity standards for IoT components, systems, and related services. The report focuses on five IoT areas: connected vehicles, consumer devices, health devices, smart buildings and smart manufacturing.

3. APPLICABLE LAWS (EXEMPLARY)

a. FTC Authority and Oversight

i. The FTC's enforcement authority is derived from over 70 different statutes, including the Federal Trade Commission Act.[6] Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45 ("Section 5"), authorizes the FTC to bring actions—in both judicial and administrative forums—against entities engaging in "unfair or deceptive acts or practices in or affecting commerce."[7]

ii. The FTC interprets its Section 5 authority as allowing it to regulate—and to bring enforcement actions related to—allegedly unfair or deceptive acts or practices in the data privacy and security arena. The FTC has become the leading federal regulatory authority on privacy and security, and has brought many cases against companies allegedly engaged in unfair or deceptive practices that put consumers' personal data at unreasonable risk.

iii. An August 24, 2015 decision by the Third Circuit Court of Appeals in *FTC v. Wyndham Worldwide Corporation*[8] recognized—for the first time by a U.S.

---

[4] https://www.nist.gov/cyberframework.

[5] https://doi.org/10.6028/NIST.IR.8200.

[6] 15 U.S.C. §§ 41-58.

[7] *See generally In the Matter of CardSystems Solutions, Inc. et al.*, FTC Dkt. No. C-4168 (Sept. 5, 2006) (complaint); *In the Matter of DSW, Inc.*, FTC Dkt. No. C-4157 (Mar. 7, 2006) (complaint); *United States v. ChoicePoint, Inc.*, No. 106-cv-0198, Dkt. No. 5 (N.D. Ga. Feb. 15, 2006) (stipulated judgment); *In the Matter of BJ's Wholesale Club, Inc*., FTC Dkt. No. C-4148 (Sept. 20, 2005) (complaint).

[8] *FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

appellate court—that the FTC has authority to regulate "unfair" or "deceptive" cybersecurity practices under Section 5.

iv. On June 6, 2018, the Eleventh Circuit in *LabMD, Inc. v. Federal Trade Commission* vacated a cease and desist order by the FTC Commission directing LabMD to create and implement a variety of protective measures.[9] The Court did not question the FTC's authority under Section 5 to oversee cybersecurity and privacy practices, but it challenged the FTC's practice of demanding that defendants institute "reasonable" security practices, and found that such orders must "enjoin a specific act or practice."

v. The FTC also has specific enforcement authority for data privacy under statutes such as COPPA, FCRA, HITECH (breach notice). In June 2017, the FTC updated its COPPA Guidance to explicitly note that the statutes reference to "[w]ebsite or online service" includes "connected toys or other Internet of Things devices."[10]

b. U.S. Consumer Product Safety Commission ("CPSC")

i. The CPSC held a hearing in May 2018 on IoT product safety, but focused on risks of physical injury rather than data privacy.[11] The hearing followed a 2017 staff report on the safety risks associated with many new technologies, including IoT.[12]

c. State laws

i. <u>*Consumer Protection*</u>: States have broad consumer protection statutes, typically in the form of Unfair and Deceptive Trade Practices Acts ("UDTPAs"). These laws are often modeled after Section 5(a) of the FTC Act, prohibiting trade practices that are "unfair" or "deceptive." Like the FTC, state attorneys general ("AGs") leverage these laws to pursue companies

[9] *LabMD, Inc. v. Federal Trade Commission*, 894 F.3d 1221 (11th Cir. 2018).

[10] FTC, *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business* (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance.

[11] CPSC, *The Internet of Things and Consumer Products Hazards*, 83 Fed. Reg. 13122 (Mar. 27, 2018).

[12] CPSC, Staff Report, *Potential Hazards Associated with Emerging and Future Technologies* (Jan. 19, 2017), https://www.cpsc.gov/content/potential-hazards-associated-with-emerging-and-future-technologies.

for unsatisfactory data privacy and security practices, frequently after a reported data incident. UDTPAs can provide a variety of remedies to state attorneys general such as injunctions, restitution, and civil penalties. Similarly, civil penalties can range up to $50,000 per violation.[13] Some jurisdictions have held that a civil penalty may be imposed *for each individual violation* of a consumer protection statute.[14] In addition, at least 26 states and the District of Columbia permit an individual to bring a private right of action to recover damages or obtain equitable relief from businesses for injuries from a cyber-incident, for failure to notify customers of a breach in a timely manner, or under state consumer protection statutes such as UDTPAs.[15] In some cases, prevailing plaintiffs are permitted to recover reasonable attorney's fees and court costs.

ii. <u>*Data privacy*</u>: As of January 1, 2020, the California Consumer Privacy Act of 2018 ("CCPA") will create at least four core individual rights for consumers: (1) the right to know what PII is collected, sold, and disclosed (and to whom); (2) the right to opt-out of the sale of PII; (3) the right to deletion of PII; (4) and the right not to be discriminated against for exercising such rights. *It is unclear whether an employee will be deemed a "consumer" under the law*, but for now the statute is understood to include it. The CCPA is being viewed as "GDPR-lite" and adopts many of its concepts, including a broad definition of what constitutes PII. The CCPA is likely to undergo further revisions before 2020 and the California AG's office will be promulgating rules under the CCPA. Other states are expected to follow suit, and Congress is gearing up for a federal privacy law, but it remains unclear what that law will look like and to what extent it will preempt state laws.

---

[13] *See* Cal. Bus. & Prof. Code § 17206(a) (California Attorney General may seek civil penalty not to exceed $2,500 "for each violation"); 815 Ill. Comp. Stat. 505/7 (Illinois Attorney General can seek civil penalty not to exceed $50,000.00 "against any person found to have engaged in any method, act or practice declared unlawful under this Act" when taken "with the intent to defraud."); Me. Rev. Stat. tit. 5, § 209 (Maine Attorney General can seek civil penalty of not more than $10,000 for "each intentional violation"); Vt. Stat. Ann. tit. 9, § 2458(b)(1) (Vermont Attorney General may seek a civil penalty of not more than $10,000 "for each violation").

[14] *See McGraw v. Imperial Mktg*., 203 W. Va. 203, 219 n.6 (W.Va. Sup. Ct. 1998) (Starcher, J. concurring) (listing various state imposed penalties).

[15] For example, Florida and North Carolina, among others, have UDPTAs with private causes of action. *See* Fla. Stat. Ann. §§ 501.203, 501.211; N.C. Gen. Stat § 75-1.1; *see also In re: Target Corp. Customer Data Security Breach Litig*., 66 F.Supp.3d 1154 (D. Minn. Dec. 18, 2014) (addressing a number of state UDTPAs asserted in a class action stemming from a data breach).

iii. *IoT laws*: On September 28, 2018, California's governor signed into law the nation's first IoT bill.[16] The law will go into effect on January 1, 2020 and requires that manufacturers implement "reasonable security features" in IoT devices sold in California. The law provides certain specific requirements, such as rules for password and user authentication, its broad obligation for reasonable security presents some ambiguity for manufacturers, similar to the issues that manufacturers have complained about with respect to the FTC's enforcement of alleged Section 5 violations for unreasonable practices. Notably, the This law does not provide a private right of action and vests exclusive authority to enforce the law with the state's Attorney General and city/county prosecutors.

4. IOT ENFORCEMENT AND LEGAL ACTION (EXEMPLARY)

a. Regulatory Enforcement

i. FTC Activities

1. *TRENDnet and ASUSTeK*: The FTC has brought a number of enforcement actions for perceived failures to properly secure IoT devices. For example, it brought actions against a manufacturer of baby cameras in 2013[17] and a router manufacturer in 2016. The agency resolved both actions through consent orders that required the businesses to (i) establish security programs designed to provide consumers with secure devices; (ii) conduct security audits for 20 years; and (iii) provide audit reports to the FTC upon request.[18]

2. *VTech*: In January 2018 the FTC brought an enforcement actions against Vtech for a connected toy app alleged to have collected children's personal information without parental consent, in violation of COPPA and FTC Act—the parties entered into a stipulated order under which Vtech paid $650,000 and agreed to a number of data privacy and security compliance and reporting obligations.[19]

[16] Senate Bill 327; Assembly Bill 1906.

[17] *In the Matter of TRENDnet INC.*, FTC Dkt. No. C-4426, Decision and Order (Jan. 16, 2014).

[18] *In the Matter of ASUSTeK Computer Inc.*, FTC Dkt. No. C-4587, Decision and Order (July 18, 2016).

[19] *USA v. Vtech Elec. Ltd. et al.*, No. 1:18-cv-114 (N.D. Ill. Jan. 8, 2018)

3. *Vizio*: On February 6, 2017, the FTC announced that Vizio would pay $2.2 million to the FTC and State of New Jersey to settle charges it collected viewing histories on 11 million smart televisions without users' consent. The stipulated consent order also required Vizio to provide clear representations about its privacy practices, obtain affirmative consent for its data collection and sharing practices, delete data collected before March 1, 2016, and implement a comprehensive data privacy program with biennial assessments.[20]

4. *D-Link*: In January 2017, the FTC sued D-Link under Section 5 for alleged failures to reasonably secure its routers and web cameras from widely known and reasonably foreseeable security risks. The Court dismissed some but not all of the FTC's claims on September 19, 2017 following D-Link's motion to dismiss. On September 21, 2018, the FTC and D-Link Systems Inc. each filed a motion for summary judgement.[21] The dispute, which dates back to early 2017, concerns alleged may have widespread implications on companies' potential liability for lax security practices, even in the absence of actual consumer harm..

ii. State AGs

1. *Safetech*: On May 22, 2017, the New York Attorney General announced a settlement with Safetech over allegations that it sold insecure IoT door locks and padlocks. According to the agreement, Safetech would have to encrypt all passwords and other credentials in their IoT devices, prompt users to change default passwords upon setup, and implement a written comprehensive security program to address security in the products. At the time the NY AG noted it was the first AG enforcement action against a company for poor IoT security practices.[22]

---

[20] *FTC. v. Vizio, Inc. et al.*, No. 2:17-cv-00758, Stipulated Order For Permanent Injunction and Monetary Judgment (D. N.J. Feb. 6, 2017); Press Release, VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent (Feb. 6, 2017), https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

[21] *FTC v. D-Link Systems Inc.*, No. 3:17-cv-00039 (N.D. Cal.)

[22] Press Release, *A.G. Schneiderman Announces Settlement With Tech Company Over Sale Of Insecure Bluetooth Door And Padlocks* (May 22, 2017), https://ag.ny.gov/press-release/ag-

5. CIVIL CASES AND CLASS ACTIONS

i. *Kyle Zak et al v. Bose Corp.*: Class action filed against Bose on April 18, 2017 alleging its products collect users' music and audio selections and disclose it to a third party data miner for analysis. Bose's motion to dismiss is pending.[23]

ii. *P. v. Standard Innovation (US), Corp.*: In early 2017, a manufacturer of mobile app-controlled vibrator devices agreed to pay $3.75 million to settle a privacy class action alleging that its devices secretly collected intimate information from users such as when and on what settings the device was used.[24] Standard also agreed to stop collecting the information and destroy the data it already collected.

iii. *Ross v St Jude Medical Inc.*: One day after an infamous report from Muddy Water Capital was released with alleged "security vulnerabilities" in St Jude cardiac devices, a patient filed a class action based on the allegations.[25] The case was subsequently dropped by the plaintiff.

iv. *ADT cases*: In 2014, home security company ADT was sued for allegedly insecure security systems that could be hacked and allow third parties to disable security features or "use customers' own security cameras to unknowingly spy on them."[26] The plaintiff alleged that his system was hacked at least twice. Rather than allege specific harm, the allegations focused on ADT's marketing statements and asserted claims for fraud, strict product liability and unjust enrichment. After lengthy discovery, various

---

schneiderman-announces-settlement-tech-company-over-sale-insecure-bluetooth-door; *In the Matter of Investigation of Safetech Products, LLC et al.*, Assurance No. 17-056, Attorney General of the State of New York (May 9, 2017).

[23] *Kyle Zak et al v. Bose Corp.*, No. 1:17-cv-02928, Class Action Complaint (N.D. Ill. Apr. 18, 2017).

[24] *P. v. Standard Innovation (US), Corp.*, No. 1:16-cv-08655, DKt. 27, Plaintiffs' Motion For And Memorandum In Support Of Preliminary Approval Of Class Action Settlement (N.D. Ill. Mar. 9, 2017).

[25] *Ross v St Jude Medical Inc.*, No 2:16- cv-06465 (CD Cal 2016).

[26] *Baker v. The ADT Corporation et al.*, No. 2:15-cv-02038 (C.D. Ill.).

parties agreed to a nationwide settlement under which ADT would pay $16 million for class counsel legal fees and customer awards of $15 to $45.[27]

v. *In re Visio*: Concurrent with resolution of the FTC and state AG investigations concerning data-tracking software installed on Vizio smart TVs, on October 4, 2018 Vizio filed a motion for approval to settle the consumer class actions consolidated California federal court fir $17 million. Vizio also agreed to revise on-screen disclosures concerning its viewing data practices.[28]

vi. *Flynn v FCA US LLC*.: Although more of a cybersecurity case than a privacy case, a federal court recently held that a class action case filed in 2015 and alleging that Fiat Chrysler designed and installed defective "Uconnect" infotainment systems that could be hacked and remotely controlled would proceed to trial.[29]

6. IoT IN OTHER LEGAL CONTEXTS

a. *Witness to murder?* On November 5, 2018, a court in New Hampshire ordered Amazon to produce two days of recordings from an Amazon Echo device suspected of capturing audio at the time a double murder occurred in the location.[30]

b. *Pacemaker subverts insurance fraud*: Police questioning an individual about a fire that caused about $400,000 in damages at his home were told that when he

---

[27] *Edenborough et al. v. ADT, LLC et al*., No. 3:16-cv-02233, Dkt. 94, Plaintiffs' Notice Of Motion, Unopposed Motion, And Memorandum In Support Of Preliminary Approval Of Class Action Settlement (N.D. Cal. Mar. 23, 2017).

[28] *In Re: Vizio, Inc., Consumer Privacy Litigation*, No. 8:16-ml-02693, Dkt. 282-1 (C.D. Cal. Oct. 4, 2018).

[29] *Flynn v FCA US LLC*, No. 3:15-cv-00855, Dkt. 411, Memorandum & Order (S.D. Ill. Oct. 9, 2018). The Court previously found there existed a genuine dispute as to whether the class vehicles had defects, whether the alleged defects were remedied by the recall and whether additional measures were required to protect the vehicles from an unreasonable risk of hacking. Specifically, the plaintiffs' warranty and fraudulent misrepresentation claims survived a summary judgment motion, and the Court granted class certification but limited it to the named plaintiffs' states (Michigan, Illinois and Missouri). Another car hacking case filed around the same time was dismissed by the Court. *See Cahen v. Toyota Motor Corp*., 3:15-cv-01104 (N.D. Cal. March 10, 2015).

[30] *State of New Hampshire v. Verrill*, No. 219-2017-cr-072, Order on Motion to Search in Lieu of Search Warrant (Sup. Ct. Nov. 5, 2018).

discovered the fire he gathered belongings, put them in various bags, broke out a bedroom window with his cane, threw his bags outside, and rushed out of the house. But when the police reviewed data from the 59-year old's pacemaker, it showed that his heart rate barely changed during the fire. After a cardiologist testified that the man's story was "highly improbable" under the circumstances he was charged with arson and insurance fraud.[31]

[31] Journal News, *Data from man's pacemaker led to arson charges* (Jan 27, 2017), https://www.journal-news.com/news/data-from-man-pacemaker-led-arson-charges/sDp2XXGPY1EKJkY57sureP/; WLWT-TV, *Ross Compton indicted on charges of arson, insurance fraud* (Jan. 27, 2017), https://www.wlwt.com/article/middletown-mans-electronic-heart-monitor-leads-to-his-arrest/8647942.

U.S. Department of Homeland Security

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

Version 1.0

November 15, 2016

INTRODUCTION AND OVERVIEW

The growth of network-connected devices, systems, and services comprising the Internet of Things (IoT)[1] creates immense opportunities and benefits for our society. IoT security, however, has not kept up with the rapid pace of innovation and deployment, creating substantial safety and economic risks. This document explains these risks and provides a set of non-binding principles and suggested best practices to build toward a responsible level of security for the devices and systems businesses design, manufacture, own, and operate.

Growth and Prevalence of the Internet of Things

Internet-connected devices enable seamless connections among people, networks, and physical services. These connections afford efficiencies, novel uses, and customized experiences that are attractive to both manufacturers and consumers. Network-connected devices are already becoming ubiquitous in, and even essential to, many aspects of day-to-day life, from fitness trackers, pacemakers, and cars, to the control systems that deliver water and power to our homes. The promise offered by IoT is almost without limit.

Prioritizing IoT Security

While the benefits of IoT are undeniable, the reality is that security is not keeping up with the pace of innovation. As we increasingly integrate network connections into our nation's critical infrastructure, important processes that once were performed manually (and thus enjoyed a measure of immunity against malicious cyber activity) are now vulnerable to cyber threats. Our increasing national dependence on network-connected technologies has grown faster than the means to secure it.

The IoT ecosystem introduces risks that include malicious actors manipulating the flow of information to and from network-connected devices or tampering with devices themselves, which can lead to the theft of sensitive data and loss of consumer privacy, interruption of business operations, slowdown of internet functionality through large-scale distributed denial-of-service attacks, and potential disruptions to critical infrastructure.

Last year, in a cyber attack that temporarily disabled the power grid in parts of Ukraine, the world saw the critical consequences that can result from failures in connected systems. Because our nation is now dependent on properly functioning networks to drive so many life-sustaining activities, IoT security is now a matter of homeland security.

[1] In this context, the term IoT refers to the connection of systems and devices with primarily physical purposes (e.g. sensing, heating/cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems.

It is imperative that government and industry work together, quickly, to ensure the IoT ecosystem is built on a foundation that is trustworthy and secure. In 2014, the President's National Security Telecommunications Advisory Committee (NSTAC) highlighted the need for urgent action.

> IoT adoption will increase in both speed and scope, and [will] impact virtually all sectors of our society. The Nation's challenge is ensuring that the IoT's adoption does not create undue risk. Additionally…. there is a small—and rapidly closing—window to ensure that IoT is adopted in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations.[2]

The time to address IoT security is right now. This document sets the stage for engagement with the public and private sectors on these key issues. It is a first step to motivate and frame conversations about positive measures for IoT security among IoT developers, manufacturers, service providers, and the users who purchase and deploy the devices, services, and systems. The following principles and suggested practices provide a strategic focus on security and enhance the trust framework that underpins the IoT ecosystem.

Overview of Strategic Principles

Many of the vulnerabilities in IoT could be mitigated through recognized security best practices, but too many products today do not incorporate even basic security measures. There are many contributing factors to this security shortfall. One is that it can be unclear who is responsible for security decisions in a world in which one company may design a device, another supplies component software, another operates the network in which the device is embedded, and another deploys the device. This challenge is magnified by a lack of comprehensive, widely-adopted international norms and standards for IoT security. Other contributing factors include a lack of incentives for developers to adequately secure products, since they do not necessarily bear the costs of failing to do so, and uneven awareness of how to evaluate the security features of competing options.

The following principles, set forth in the next section, offer stakeholders a way to organize their thinking about how to address these IoT security challenges:

- Incorporate Security at the Design Phase
- Advance Security Updates and Vulnerability Management
- Build on Proven Security Practices

[2] National Security Telecommunications Advisory Committee Report to the President on the Internet of Things, November 19, 2014.

Prioritize Security Measures According to Potential Impact

Promote Transparency across IoT

Connect Carefully and Deliberately

As with all cybersecurity efforts, IoT risk mitigation is a constantly evolving, shared responsibility between government and the private sector. Companies and consumers are generally responsible for making their own decisions about the security features of the products they make or buy. The role of government, outside of certain specific regulatory contexts and law enforcement activities, is to provide tools and resources so companies, consumers, and other stakeholders can make informed decisions about IoT security.

Scope, Purpose, and Audience

The purpose of these non-binding principles is to equip stakeholders with suggested practices that help to account for security as they develop, manufacture, implement, or use network-connected devices. Specifically, these principles are designed for:

1	**IoT developers** to factor in security when a device, sensor, service, or any component of the IoT is being designed and developed;
2	**IoT manufacturers** to improve security for both consumer devices and vendor managed devices;
3	**Service providers,** that implement services through IoT devices, to consider the security of the functions offered by those IoT devices, as well as the underlying security of the infrastructure enabling these services; and
4	**Industrial and business-level consumers** (including the federal government and critical infrastructure owners and operators) to serve as leaders in engaging manufacturers and service providers on the security of IoT devices.

STRATEGIC PRINCIPLES FOR SECURING IOT

The principles set forth below are designed to improve security of IoT across the full range of design, manufacturing, and deployment activities. Widespread adoption of these strategic principles and the associated suggested practices would dramatically improve the security posture of IoT. There is, however, no one-size-fits-all solution for mitigating IoT security risks. Not all of the practices listed below will be equally relevant across the diversity of IoT devices. These principles are intended to be adapted and applied through a risk-based approach that takes into account relevant business contexts, as well as the particular threats and consequences that may result from incidents involving a network-connected device, system, or service.

Incorporate Security at the Design Phase

Security should be evaluated as an integral component of any network-connected device. While there are exceptions, in too many cases economic drivers or lack of awareness of the risks cause businesses to push devices to market with little regard for their security. Building security in at the design phase reduces potential disruptions and avoids the much more difficult and expensive endeavor of attempting to add security to products after they have been developed and deployed. By focusing on security as a feature of network-connected devices, manufacturers and service providers also have the opportunity for market differentiation. The practices below are some of the most effective ways to account for security in the earliest phases of design, development, and production.

What are the potential impacts of not building security in during design?

Failing to design and implement adequate security measures could be damaging to the manufacturer in terms of financial costs, reputational costs, or product recall costs. While there is not yet an established body of case law addressing IoT context, traditional tort principles of product liability can be expected to apply.

SUGGESTED PRACTICES:

Enable security by default through unique, hard to crack default user names and passwords. User names and passwords for IoT devices supplied by the manufacturer are

often never changed by the user and are easily cracked. Botnets operate by continuously scanning for IoT devices that are protected by known factory default user names and passwords. Strong security controls should be something the industrial consumer has to deliberately disable rather than deliberately enable.

Build the device using the most **recent operating system** that is technically viable and economically feasible. Many IoT devices use Linux operating systems, but may not use the most up-to-date operating system. Using the current operating system ensures that known vulnerabilities will have been mitigated.

Use **hardware that incorporates security features** to strengthen the protection and integrity of the device. For example, use computer chips that integrate security at the transistor level, embedded in the processor, and provide encryption and anonymity.

Design with system and operational disruption in mind. Understanding what consequences could flow from the failure of a device will enable developers, manufacturers, and service providers to make more informed risk-based security decisions. Where feasible, developers should build IoT devices to fail safely and securely, so that the failure does not lead to greater systemic disruption.

Promote Security Updates and Vulnerability Management

Even when security is included at the design stage, vulnerabilities may be discovered in products after they have been deployed. These flaws can be mitigated through patching, security updates, and vulnerability management strategies. In designing these strategies, developers should consider the implications of a device failure, the durability of the associated product, and the anticipated cost of repair. In the absence of the ability to deploy security updates, manufacturers may be faced with the decision between costly recalls and leaving devices with known vulnerabilities in circulation.

FOCUS ON: NTIA Multi-Stakeholder Process on Patching and Updating

The National Telecommunications and Information Administration (NTIA) has convened a multi-stakeholder process concerning the "Internet of Things Upgradability and Patching" to bring stakeholders together to share the range of views on security upgradability and patching, and to establish more concrete goals for industry-wide adoption.

SUGGESTED PRACTICES:

Consider ways in which to **secure the device over network connections or through automated means**. Ideally, patches would be applied automatically and leverage cryptographic integrity and authenticity protections to more quickly address vulnerabilities.

Consider **coordinating software updates among third-party vendors** to address vulnerabilities and security improvements to ensure consumer devices have the complete set of current protections.

Develop **automated mechanisms for addressing vulnerabilities**. In the software engineering space, for example, there are mechanisms for ingesting information from critical vulnerability reports sourced from the research and hacker communities in real time. This allows developers to address those vulnerabilities in the software design, and respond when appropriate.

Develop a policy regarding the **coordinated disclosure of vulnerabilities**, including associated security practices to address identified vulnerabilities. A coordinated disclosure policy should involve developers, manufacturers, and service providers, and include information regarding any vulnerabilities reported to a computer security incident response team (CSIRT). The US Computer Emergency Readiness Team (US-CERT), Industrial Control Systems (ICS)-CERT, and other CSIRTs provide regular technical alerts, including after major incidents, which provide information about vulnerabilities and mitigation.

Develop an **end-of-life strategy** for IoT products. Not all IoT devices will be indefinitely patchable and updateable. Developers should consider product sunset issues ahead of time and communicate to manufacturers and consumers expectations regarding the device and the risks of using a device beyond its usability date.

Build on Recognized Security Practices

Many tested practices used in traditional IT and network security can be applied to IoT. These approaches can help identify vulnerabilities, detect irregularities, respond to potential incidents, and recover from damage or disruption to IoT devices.

FOCUS ON: NIST Cybersecurity Risk Management Framework

The National Institute of Standards and Technology (NIST) published a framework for cybersecurity risk management that has been widely adopted by private industry, integrated across sectors, and within organizations. The framework is widely recognized as a comprehensive touchstone for organizational cyber risk management https://www.nist.gov/cyberframework. While not specific to IoT, the risk framework provides a starting point for considering risks and best practices.

SUGGESTED PRACTICES:

Start with **basic software security and cybersecurity practices** and apply them to the IoT ecosystem in flexible, adaptive, and innovative ways.

Refer to relevant **Sector-Specific Guidance**, where it exists, as a starting point from which to consider security practices. Some federal agencies address security practices for the unique sectors that they regulate. For example, the National Highway Traffic Safety Administration (NHTSA) recently released guidance on Cybersecurity Best Practices for Modern Vehicles that address some of the unique risks posed by autonomous or semi-autonomous vehicles. Similarly, the Food and Drug Administration released draft guidance on Postmarket Management of Cybersecurity in Medical Devices.

Practice defense in depth. Developers and manufacturers should employ a holistic approach to security that includes layered defenses against cybersecurity threats, including user-level tools as potential entry points for malicious actors. This is especially valuable if patching or updating mechanisms are not available or insufficient to address a specific vulnerability.

Participate in **information sharing platforms** to report vulnerabilities and receive timely and critical information about current cyber threats and vulnerabilities from public and private partners. Information sharing is a critical tool in ensuring stakeholders are aware of threats as they arise[3]. The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), as well as multi-state and sector-specific information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs), are examples.

[3] "Information Sharing," National Cybersecurity and Communications Information Center.

Prioritize Security Measures According to Potential Impact

Risk models differ substantially across the IoT ecosystem. For example, industrial consumers (such as nuclear reactor owners and operators) will have different considerations than a retail consumer. The consequences of a security failure across different customers will also vary significantly. Focusing on the potential consequences of disruption, breach, or malicious activity across the consumer spectrum is therefore critical in determining where particular security efforts should be directed, and who is best able to mitigate significant consequences.

Should IoT security measures focus on the IoT device?

Since the purpose of all IoT processes is to take in information at a physical point and motivate a decision based on that information (sometimes with physical consequences), security measures can focus on one or more parts of the IoT process. As noted earlier, the risks to IoT begin with the specific device, but are certainly not limited to it. Developers, manufacturers, and service providers should consider specific risks to the IoT device as well as process and service, and make decisions based on relative impact to all three as to where the most robust measures should be applied.

SUGGESTED PRACTICES:

Know a device's **intended use and environment**, where possible. This awareness helps developers and manufacturers consider the technical characteristics of the IoT device, how the device may operate, and the security measures that may be necessary.

Perform a "**red-teaming" exercise**, where developers actively try to bypass the security measures needed at the application, network, data, or physical layers. The resulting analysis and mitigation planning should help prioritize decisions on where and how to incorporate additional security measures.

Identify and authenticate the devices connected to the network, especially for industrial consumers and business networks. Applying authentication measures for known devices and services allows the industrial consumer to control those devices and services that are within their organizational frameworks.

Promote Transparency across IoT

Where possible, developers and manufacturers need to know their supply chain**,** namely, whether there are any associated vulnerabilities with the software and hardware components provided by vendors outside their organization. Reliance on the many low-cost, easily accessible software and hardware solutions used in IoT can make this challenging. Because developers and manufactures rely on outside sources for low-cost, easily accessible software and hardware solutions, they may not be able to accurately assess the level of security built into component parts when developing and deploying network-connected devices. Furthermore, since many IoT devices leverage open source packages, developers and manufacturers many not be able to identify the sources of these component parts.

Increased awareness could help manufacturers and industrial consumers identify where and how to apply security measures or build in redundancies. Depending on the risk profile of the product in question, developers, manufacturers, and service providers will be better equipped to appropriately mitigate threats and vulnerabilities as expeditiously as possible, whether through patching, product recall, or consumer advisory.

SUGGESTED PRACTICES:

Conduct end-to-end risk assessments that account for both internal and **third party vendor risks,** where possible. Developers and manufacturers should include vendors and suppliers in the risk assessment process, which will create transparency and enable them to gain awareness of potential third-party vulnerabilities and promote trust and transparency. Security should be readdressed on an ongoing basis as the component in the supply chain is replaced, removed or upgraded.

Consider creating a **publicly disclosed mechanism for using vulnerability reports**. Bug Bounty programs, for example, rely on crowdsourcing methods to identify vulnerabilities that companies' own internal security teams may not catch.

Consider developing and employing a **software bill of materials** that can be used as a means of building shared trust among vendors and manufacturers. Developers and manufacturers should consider providing a list of known hardware and software components in the device package in a manner which is mindful of the need to protect intellectual property issues. A list can serve as valuable tool for others in the IoT ecosystem to understand and manage their risk and patch any vulnerabilities immediately following any incident.

Connect Carefully and Deliberately

IoT consumers, particularly in the industrial context, should deliberately consider whether continuous connectivity is needed given the use of the IoT device and the risks associated with its disruption. IoT consumers can also help contain the potential threats posed by network connectivity by connecting carefully and deliberately, and weighing the risks of a potential breach or failure of an IoT device against the costs of limiting connectivity to the Internet.

In the current networked environment, it is likely that any given IoT device may be disrupted during its lifecycle. IoT developers, manufacturers, and consumers should consider how a disruption will impact the IoT device's primary function and business operations following the disruption.

Does every networked device need continuous, automated connection to the Internet?

In 2015, the Federal Trade Commission published a guide called "Start with Security: A Guide for Businesses" to help them determine this very question. While it may be convenient to have continuous network access, it may not be necessary for the purpose of the device – and systems; for example, nuclear reactors, where a continuous connection to the internet opens up the opportunity for an intrusion of potentially enormous consequences.

SUGGESTED PRACTICES:

Advise IoT consumers on the intended purpose of any network connections. Direct internet connections may not be needed to operate critical functions of an IoT device, particularly in the industrial setting. Information about the nature and purpose of connections can inform consumer decisions.

Make intentional connections. There are instances when it is in the consumer's interest not to connect directly to the Internet, but instead to a local network that can aggregate and evaluate any critical information. For example, Industrial Control Systems (ICS) should be protected through defense in depth principles as published by https://ics-cert.us-cert.gov/recommended_practices.

Build in controls to allow manufacturers, service providers, and consumers to disable network connections or specific ports when needed or desired to enable **selective connectivity**. Depending on the purpose of the IoT device, providing the consumers with guidance and control over the end implementation can be a sound practice.

CONCLUSION

Our nation cannot afford a generation of IoT devices deployed with little consideration for security. The consequences are too high given the potential for harm to our critical infrastructure, our personal privacy, and our economy.

As DHS issues these principles, we recognize the efforts underway by our colleagues at other federal agencies, and the work of private sector entities to advance architectures and institute practices to address the security of the IoT. This document is a first step to strengthen those efforts by articulating overarching security principles. But next steps will surely be required.

DHS identifies four lines of effort that should be undertaken across government and industry to fortify the security of the IoT.

FOUR LINES OF EFFORT:

1 

Coordinate across federal departments and agencies to engage with IoT stakeholders and jointly explore ways to mitigate the risks posed by IoT.
DHS with its federal partners will continue to engage with industry partners to determine approaches that can further enhance IoT security, and to promote understanding of evolving technology trends that may address IoT risks. Future efforts will also focus on updating and applying these principles, as best practices and approaches are further refined and understood.

2 

Build awareness of risks associated with IoT across stakeholders.
It is important that stakeholders are aware of IoT risks so that they can position themselves to address them. DHS will accelerate public awareness, education, and training initiatives, in partnership with other agencies, the private sector, and international partners. DHS, together with other agencies, will also undertake initiatives more directly tailored to particular sectors and individual consumers.

3 

Identify and advance incentives for incorporating IoT security.
Policymakers, legislators, and stakeholders need to consider ways to better incentivize efforts to enhance the security of IoT. In the current environment, it is too often unclear who bears responsibility for the security of a given product or system. In addition, the costs of poor security are often not borne by those best positioned to increase security. DHS and all other stakeholders need to consider

how tort liability, cyber insurance, legislation, regulation, voluntary certification management, standards-settings initiatives, voluntary industry-level initiatives, and other mechanisms could improve security while still encouraging economic activity and groundbreaking innovation. Going forward, DHS will convene with partners to discuss these critical matters and solicit ideas and feedback.

4 

Contribute to international standards development processes for IoT.
IoT is part of a global ecosystem, and other countries and international organizations are beginning to evaluate many of these same security considerations. It is important that IoT-related activities not splinter into inconsistent sets of standards or rules. As DHS becomes increasingly focused on IoT efforts, we must engage with our international partners and the private sector to support the development of international standards and ensure they align with our commitment to fostering innovation and promoting security.

DHS looks forward to these next collaborative steps. Together, we can, and must, address these complex challenges. By doing so, we will ensure that our network-connected future is not only innovative, but also secure and built to last.

APPENDIX: GUIDANCE AND ADDITIONAL RESOURCES

The principles in this document have been developed based on information gathered from industry reports, and through discussions with private industry, trade associations, non-governmental entities, and Federal partners, especially with NIST and NTIA.

Department of Homeland Security

- https://www.dhs.gov/sites/default/files/publications/draft-lces-security-comments-508.pdf
- https://www.dhs.gov/publication/security-tenets-lces
- https://www.dhs.gov/sites/default/files/publications/security-tenets-lces-paper-11-20-15-508.pdf

Other Federal Entities

- National Security Telecommunications Advisory Committee
    1. Final NSTAC Internet of Things Report

- NTIA
    1. Notice and Request for Comments on the Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things
        a) Comments
    2. Green Paper – Cybersecurity, Innovation and the Internet Economy, 2011
    3. New Insights into the Emerging Internet of Things
    4. Remarks of Deputy Assistant Secretary Simpson at Fostering the Advancement of the Internet of Things Workshop, 9/9/2016
        a) Announcement for Fostering the Advancement of the Internet of Things Workshop
    5. Internet Policy Task Force resource/review/cataloging of the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things.

- NIST
    1. Cybersecurity Framework
    2. Cyber-Physical Systems (CPS) Program
        a) CPS Public Working Group (PWG) draft Cyber-Physical Systems (CPS) Framework Release 1.0
            o Comments accepted through 9/2/2015

3. Smart-Grid Program
4. International Technical Working Group on IoT-Enabled Smart City Framework
5. NIST Special Publication (SP) 800-183, Network of Things, 7/28/2016.
    a) NIST news release

- Federal Trade Commission
    1. FTC Staff Report, "Internet of Things: Privacy & Security in a Connected World," January 2015.

- United States Congress
    1. Senate Committee on Commerce, Science, and Transportation committee hearing, "The Connected World: Examining the Internet of Things."
    2. Senate unanimously bipartisan resolution (S. Res. 110) calling for a national strategy to guide the development of the Internet of Things.
    3. House Energy and Commerce Committee's "The Internet of Things: Exploring the Next Technology Frontier"
- Government Accounting Office
    1. GAO engagement with DHS: GAO is currently engaged with DHS on IoT, code 100435 [January 15, 2016 notification letter available via this link]
        a) Status/entry in the most recent, June 3, 2016 List of Active GAO Engagements Related to DHS

External Sources

The list of additional resources is provided solely as a reference and does not constitute an endorsement by the Department of Homeland Security (DHS). DHS does not endorse any commercial product, service, or enterprise.

- Atlantic Council
    1. Smart Homes and the Internet of Things – http://www.atlanticcouncil.org/publications/issue-briefs/smart-homes-and-the-internet-of-things
- I Am The Cavalry
    1. Five Star Automotive Cyber Safety Framework – https://iamthecavalry.org/5star
    2. Hippocratic Oath for Connected Medical Devices – https://iamthecavalry.org/oath
- Online Trust Alliance
    1. Consumer Best Practices
- Industrial Internet Consortium: http://www.iiconsortium.org/IISF.htm
- Open Web Application Security Project (OWASP)

1. Internet of Things Project
   https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
2. Internet of Things Security Guidance
   https://www.owasp.org/index.php/IoT_Security_Guidance

- Safecode.org relevant industry best practices www.safecode.org
- AT&T
  1. Exploring IoT Security
- Symantec
  1. An Internet of Things Reference Architecture
     https://www.symantec.com/content/dam/symantec/docs/white-papers/iot-security-reference-architecture-en.pdf

Eric H. Gibbs (Bar No. 178658)
Andre M. Mura (Bar No. 298541)
Linda Lam (Bar No. 301461)
GIBBS LAW GROUP LLP
505 14th Street, Suite 1110
Oakland, CA 94612
Telephone: (510) 350-9700
Facsimile: (510) 350-9701
ehg@classlawgroup.com
amm@classlawgroup.com
lpl@classlawgroup.com

Joseph W. Cotchett (Bar No. 36324)
Adam J. Zapala (Bar No. 245748)
Adam J. Trott (Bar No. 275520)
COTCHETT, PITRE & McCARTHY, LLP
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Telephone: 650-697-6000
Facsimile: 650-697-0577
jcotchett@cpmlegal.com
azapala@cpmlegal.com
atrott@cpmlegal.com

Plaintiffs' Interim Co-Lead Counsel

UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA SANTA ANA DIVISION

IN RE: VIZIO, INC., CONSUMER PRIVACY LITIGATION This document relates to: ALL ACTIONS	Case No. 8:16-ml-02693- JLS (KESx) **PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT OF MOTION FOR PRELIMINARY APPROVAL OF PROPOSED CLASS ACTION SETTLEMENT (UNOPPOSED)** Date: December 7, 2018 Time: 10:30 a.m. Dept: Courtroom 10-A Judge: Hon. Josephine L. Staton

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

Statutes

Rules

Other Authorities

I. Introduction

Plaintiffs seek preliminary approval of a settlement agreement providing monetary and injunctive relief for all individuals in the United States who purchased a Vizio Smart Television for personal or household use, and not for resale, that was subsequently connected to the Internet at any time between February 1, 2014 and February 6, 2017. The nationwide relief negotiated at arm's length and under the supervision of a retired federal judge, after years of intensive litigation and probing discovery, would end this multi-district litigation against Vizio on the following terms:

First, Vizio will establish a non-reversionary $17 million fund for proportional monetary payments for settlement class members who submit a claim. The fund will cover any court-approved expenses, costs, and attorneys' fees.

Second, beginning in December 2016, after this lawsuit was filed and in substantial part because of it, Vizio revised its on-screen disclosures regarding its viewing-data collection and sharing practices, in a stand-alone, on-screen disclosure, and asked for permission to collect and share viewing data. Under this settlement, Vizio will make additional changes to its on-screen disclosure for new customers and will add a disclosure to a "quick start" guide that accompanies new Smart TVs.

Third, Vizio will delete all viewing data collected during the class period which it possesses. An independent auditor will confirm that this deletion is successful.

Plaintiffs and class counsel are proud to present this settlement agreement to the Court because it is restorative. The revenue that Vizio obtained from the collection and licensing of viewing data during the class period will be fully disgorged; and in turn settlement class members will receive compensation comfortably within the range of reasonableness for their claims. Just as important, Vizio's collection of viewing data by default ended as of February 2017. Vizio's disclosures were revamped—and will be further revised as a result of this settlement. And Vizio will destroy the remaining contested viewing data in its possession.

Given the settlement's many strengths and the real risk of achieving far less after

trial, the Court should grant this unopposed motion to begin the settlement approval process.

II. Summary of Argument

All of the factors this Court must consider in determining whether to grant a motion for preliminary approval are met here.

First, it is appropriate to conditionally certify a nationwide settlement class of all individuals who purchased affected Smart TVs that were subsequently connected to the Internet during the class period. Millions of consumers purchased the affected TVs and connected them to the Internet (numerosity); questions common to all settlement class members, including whether Vizio disclosed information that would readily permit an ordinary person to identify a specific individual's video-watching behavior, are answerable through common proof (commonality); the harm that Plaintiffs have suffered is identical to the harm suffered by all settlement class members (typicality); and Plaintiffs and class counsel will continue to vigorously prosecute this litigation on behalf of the settlement class, as they have to date (adequacy).[1]

In addition, common questions predominate over any individual ones because Vizio engaged in a uniform course of conduct applicable to all settlement class members. This includes the core allegation that Vizio collected and shared viewing data during the class period without consumers' knowledge or consent. The proposed settlement class is thus sufficiently cohesive to warrant adjudication by representation. And here, because conditional certification of a single nationwide class would be based on alleged violations of federal law, there can be no argument that differences in state law defeat predominance.

Further, class adjudication is superior to other available methods of adjudication, such as individual litigation, for two reasons. The high cost of litigating this case involving complex technology overwhelms Vizio's potential liability per consumer. And the only economically rational way for litigants and the courts to resolve millions of such claims is

[1] Vizio does not oppose class certification solely for the purposes of settlement only.

through the class device.

Second, the proposed settlement is fair, reasonable, and adequate, and will likely be granted final approval. It is the product of serious, informed, non-collusive negotiations, before a former federal judge, after considerable litigation and discovery. It does not improperly grant preferential treatment to class representatives or segments of the class. It falls within the range of possible approval. And it has no obvious deficiencies. To assure the Court that preliminary approval is appropriate and final approval likely, Plaintiffs discuss herein the class definition, benefits, claims process, distribution plan (including for unclaimed funds), the scope of the release, the range of litigated outcomes, the extent of discovery, the views of Plaintiffs and counsel, the manner in which attorneys' fees will be addressed, and demonstrate there are no signs, explicit or subtle, of collusion between the parties. Plaintiffs will also seek the Court's approval of a settlement administrator.

Third, the proposed content and method of the class notice plan is sufficient. The notice program is tailored to this case and designed to maximize the number of claims from approximately 16 million class members. Affected Smart TVs that remain connected to the Internet will display a clear, concise, and plain notice to an estimated 6 million class members. That same notice will be e-mailed to an estimated 9 million class members. A custom digital and print media campaign accounting for class demographics further pushes the reach of this notice program well past the constitutional line. A long-form notice will also be available, in English and Spanish, at www.VizioTVsettlement.com, and it will answer typical questions and provide important information. Not only is this digital notice program the best practicable under the circumstances, it avoids the sizeable expense that attends first-class mail notice.

III. Overview of the Litigation

A. The alleged circumstances that prompted these lawsuits.[2]

Based in Irvine, California, Vizio has designed and sold televisions in the United

[2] Vizio's current disclosures concerning viewing data collection and licensing, which were implemented in early 2017, are described in more detail in Section IV.C.

States since 2002. This includes Internet-connected televisions, or "Smart" TVs, a key feature of which is the TV's ability to access online media content, including movies and music.

Beginning in February 2014, Vizio remotely installed automated (or automatic) content recognition software on Smart TVs that had already been sold and that did not have such software when sold. In about August 2014, Vizio began selling Smart TVs with this software pre-installed.

This technology monitors the video stream of all physical inputs and certain streamed content, by capturing real-time or near real-time data to construct a historical record of the content displayed on-screen with one-second granularity. A mathematical representation of a subsample of the viewing data, along with a unique identification number assigned to the TV, are sent to a server that operates as a match database.

More simply: Say you own a Smart TV with this software and it is connected to the Internet. You are watching a cable news program. As the program plays, the software captures certain pixels that appear on your screen and sends the mathematical representation and a unique number assigned to your TV to a computer server in the cloud. If the server has in its library this particular program,[3] then what you're watching on your Smart TV is identified; but if not, not. If there is no match, the viewing information is discarded. But if there is a match, a summary of the viewing information is stored.

In addition to capturing information about what is displayed, the software collects the TV's Internet-protocol address and WiFi signal strength, among other information. This information facilitates the delivery of advertisements to other electronic devices connected to the same network, such as a mobile device.

Why is "viewing data"—information about the content viewed on a TV and reports or data derived therefrom or combined with such data—collected? According to public

[3] The server ingests certain types of content and certain services but not pornographic material.

statements by Vizio, "the collection of viewing data can be used to generate intelligent insights for advertisers and media content providers and to drive their delivery of more relevant, personalized content to Smart TVs." Vizio, *Form S-1 Registration Statement* (July 24, 2015), at *2.[4] At one point, Vizio stated that its tracking software captures up to 100 billion data points each day from more than 10 million televisions, and "provides highly specific viewing behavior data on a massive scale with great accuracy, …" *Id.*

Vizio earns revenue by licensing this data to third parties. Decl. of Wilda Siu (identifying specific amount). Between February 1, 2014 and February 6, 2017, Vizio earned revenue that is less than the settlement amount.

During this time, the data was licensed to third parties under contracts that purport to bar them from associating viewing data with individuals or households by name or physical addresses. (Vizio does not itself associate viewing data with individuals or households by name or physical address, or share information such as name or physical address with third parties.) The contracts, however, allow third parties to associate viewing data with demographic information such as sex, age, income, marital status, and education.

Between February 2014 and February 2017, third parties licensed viewing data for three purposes: to determine in the aggregate what consumers watch and how they watch it; to analyze the effectiveness of advertising; and, starting in 2016 (after a notification was displayed on-screen referencing explicitly the delivery of target advertisements based on the collection of viewing data), to enable ad retargeting.

Consumers who purchased Smart TVs that received this tracking software through a software update were presented with a message on the TV that said:

> The VIZIO Privacy Policy has changed. Smart Interactivity has been enabled on your TV, but you may disable it in the settings menu. See www.vizio.com/privacy for more details. This message will time out in 1 minute.

[4] *Available at* https://www.sec.gov/Archives/edgar/data/1648158/000119312515262817/d946612ds1.htm.

Consumers who purchased Smart TVs with this software pre-installed also received this notice.

"Smart Interactivity" referred to the collection of viewing data. The software was on by default and operated continuously unless it was turned off by the consumer.

The settings menu of these TVs included the setting "Smart Interactivity" and the description, "Enables program offers and suggestions." Although Vizio maintains that it intended to and worked to develop certain program offers and suggestions during the class period, no program offers or suggestions were enabled for more than two years.

To turn "Smart Interactivity" off, a consumer would have had to find this setting in the menu, click on it, and then click again to disable it.

Between approximately Fall 2015 and Summer 2016, consumers whose Smart TVs had ACR software installed received a new notice stating:

> Select Reset & Admin in System to disable the collection and analysis of viewing history from this television ("Smart Interactivity"). NEW: Smart Interactivity may enable the delivery of tailored ads based upon viewing history to smartphones or other devices that share an IP address or other non-personal identifiers with the television.

B. An abbreviated history of these legal proceedings.

In November 2015, investigative journalists at ProPublica reported that Vizio Smart TVs collect and share customers' viewing habits with advertisers. Class action complaints were filed apace and later centralized for pre-trial proceedings in this Court.

Upon centralization here, the Court appointed interim co-lead counsel and a steering committee for Plaintiffs, as well as lead counsel for Defendants; denied a request by Vizio to stay discovery until the pleadings were set; and issued a case management schedule.

In August 2016, Plaintiffs filed a consolidated class action complaint against several Vizio entities on behalf of a nationwide class of individuals who purchased affected Smart TVs, and on behalf of subclasses of individuals from California, Florida, Massachusetts, New York, and Florida. The complaint asserted a variety of federal and state privacy

claims, and state consumer protection claims. The common thread linking all of these claims was the allegation that "Vizio offered Smart TVs equipped with automatic content recognition software that collected consumers' viewing histories and then sold that information—along with 'highly specific' information about consumers' digital identities—to third parties, without consumers' knowledge or consent." Order Denying Mot. for Interlocutory Appeal at 2.

Vizio responded to the complaint by moving to dismiss. After the Court received outsized briefing and held oral argument, it granted and denied the motion in part, allowing Plaintiffs the opportunity to replead any dismissed claim.

In March 2017, Plaintiffs filed a second consolidated complaint. Vizio again moved to dismiss. It argued that Plaintiffs' claims for injunctive relief were moot because Vizio had entered into a consent decree with the Federal Trade Commission in February 2017 that required Vizio to change its business practices relating to the collection of viewing data. Vizio also contested certain legal claims as insufficiently pleaded, and it asked the Court to strike the class definition in the second consolidated complaint because it included consumers who might be bound by arbitration agreements that forbid class proceedings in any forum.

After briefing and oral argument, the Court denied Vizio's motion in full. Vizio then filed an answer to the second consolidated complaint in August 2017. A few months later, the Court refused Vizio's separate request to certify an immediate appeal on questions of law pertaining to Vizio's liability under the federal Video Privacy Protection Act.

As things stand, Dieisha Hodges and Rory Zufolo of California; John Walsh of Massachusetts; Chris Rizzitello of New York; Linda Thomson of Washington; and Mark Queenan of Florida are named Plaintiffs for the nationwide class and their respective state sub-classes.

The Defendants named in the operative pleadings are Vizio, Inc., Vizio Holdings, Inc., Vizio Inscape Technologies, LLC; and Vizio Inscape Services, LLC. Their roles are

as follows. Vizio, Inc. is the primary Vizio entity for consumer electronics, such as Smart TVs. Vizio Holdings, Inc. was established as a holding company pending a public offering that was initiated with the filing of an S1 in July 2015 but did not advance.

Inscape Data, Inc. (formerly Vizio Inscape Technologies, LLC) (hereinafter "Inscape") develops the software on Vizio units that can recognize onscreen content, and selectively maintains a record of viewing history associated with the television. Inscape also owns the underlying automated content recognition technology, which recognizes onscreen content.[5] And Vizio Services, LLC (formerly Vizio Inscape Services, LLC) is the entity that enters into contracts with customers for Inscape viewing data.[6]

As for the parties' respective legal theories, Plaintiffs have proceeded to discovery under the Video Privacy Protection Act, Wiretap Act, California Invasion of Privacy Act, California Consumer Legal Remedies Act, California Unfair Competition Law, Florida Deceptive and Unfair Trade Practices Act, N.Y. Gen. Bus. Law § 349, Massachusetts Unfair and Deceptive Trade Practices Statute, Massachusetts Privacy Act, Washington Consumer Protection Act, unjust enrichment, intrusion upon seclusion, and fraudulent omission claims.

Vizio has denied Plaintiffs' allegations and has raised thirty-seven affirmative defenses. Vizio takes the position that it properly disclosed the collection of viewing data to consumers; that consumers consented to or had knowledge of Vizio's collection and sharing of viewing data; that the data collected by Vizio does not constitute personally identifiable information; that consumers must arbitrate their claims and cannot maintain class actions; and consumers' damages are speculative or must be judicially limited by law which proscribes damages awards that exceed actual harm.

[5] Inscape is the original Cognitive Media Networks Inc. entity. It was converted to an LLC when acquired by Vizio, Inc., and all Vizio-owned viewing data was transferred to this entity.

[6] The second consolidated complaint named Vizio Inscape Technologies, LLC and Vizio Inscape Services, LLC. The Defendants' answer to this complaint recognizes that the former is now Vizio Services, LLC, and the latter is now Inscape Data, Inc. We thus refer to these Vizio entities by their current corporate names in settlement documents and this motion.

IV. Terms of Proposed Settlement[7]

A. Proposed Settlement Class

If approved, the settlement would offer relief to the following proposed class:

> All individuals in the United States who purchased a VIZIO Smart Television for personal or household use, and not for resale, that was subsequently connected to the Internet at any time between February 1, 2014 and February 6, 2017.

Joint Decl. in Support of Motion for Preliminary Approval, Ex. 1 (hereinafter, "Settlement") ¶ I.32.

The time frame proposed corresponds with when Vizio first implemented automatic content recognition technology (February 1, 2014), and when Vizio stopped collecting viewing data through this software from Vizio Smart TVs unless the consumer affirmatively consented (February 6, 2017). Settlement ¶¶ Recitals B.10-14. Note that "viewing data" is defined in the settlement agreement to correspond with the definition of viewing data in the consent decree with the Federal Trade Commission.

All Vizio Smart TVs, including the SmartCast product line, were pre-installed with this software, or the software was installed remotely through an over-the-air update. The number of TVs with this software which connected to Vizio's servers during the class period is approximately 16 million. Assuming one purchaser per TV per household, the proposed class covers approximately 16 million individuals

The proposed settlement class definition parallels the nationwide class definition pleaded in the operative Second Consolidated Complaint (which is identical to the definition pleaded in the Consolidated Complaint). The definition proposed in these pleadings was:

> All individuals in the United States who purchased a VIZIO Smart TV with Smart Interactivity capability for personal or household use, and not for resale, during the applicable statute of limitations period.

Second Consol. Compl., Doc. 136 at ¶ 102.

[7] For readability, defined terms are not capitalized in the motion or memorandum, unless in quoted material or in the conclusion. The proposed order, by contrast, capitalizes defined terms as they appear in the settlement agreement.

The parties have made two changes to the proposed nationwide settlement class definition, neither of which affects the scope of the class. First, the proposed class definition now includes a specific date range. Second, the proposed class definition no longer refers to "Smart Interactivity capability," the Vizio's name for the automated content recognition software. Because Vizio's entire Smart TV line had this software during the class period, it is unnecessary to mention the software by name for purposes of class identification. The time period specified is sufficient to identify who is in, and who is outside of, the proposed class. The deletion of this language also improves clarity.

B. Settlement Fund

The proposed settlement contemplates a settlement fund in the amount of $17,000,000. After payment of attorneys' fees and expenses to Class Counsel, payment of the settlement administration costs, and payment of service awards, the remaining balance will be distributed proportionally to all settlement class members who submit valid claims.

The settlement fund is non-reversionary, meaning, Vizio will not be entitled to retain any part of the settlement amount that is not paid out or distributed as part of the administration of the settlement for any reason. Any part of the settlement amount that cannot feasibly be distributed to the class will be subject to a cy pres distribution to be proposed by Plaintiffs and approved by the Court.

Plaintiffs will ask the Court to award each named plaintiff up to $5,000 from the settlement fund in recognition of the time, effort, and expense they incurred pursuing claims against Vizio, which ultimately benefited the entire class. Vizio will not oppose this request. The settlement agreement preserves the Court's supervisory authority to determine the appropriateness of any service award.

Counsel will petition the Court for an award of attorneys' fees and reimbursement of costs or expenses from the settlement fund. Vizio will not oppose a request that does not exceed 33 percent of the settlement fund. The settlement agreement also preserves the Court's supervisory authority to determine the appropriateness of any such award or reimbursement.

C. Injunctive Relief

The proposed settlement provides several different forms of injunctive relief in the form of business practice changes that correspond with changes which took place during the class period pursuant to a consent decree between Vizio and the Federal Trade Commission. *See* Settlement, §§ VI, XII.

Under this consent order, Vizio agreed to display a prominent and detailed notification on the TV screen, separate and apart from any privacy policy, terms of use page, or other similar document. As part of this notification, Vizio gave consumers the option to accept viewing data collection. If a consumer opted not to accept viewing data collection, then no viewing data would be collected from the Smart TV.

Professor Joseph Turow, a leading privacy expert, was asked to review the disclosures Vizio has used since February 2017 and the disclosures proposed here, as well as contemporaneous on-screen disclosures of other smart television manufacturers whose TV sets have software that collect viewing data. He concluded that only the revised Vizio on-screen disclosures implemented with the FTC agreement:

> prominently and collectively disclose to the customer—separate from any privacy policy, terms of use page, or other similar document— four categories of information: the types of viewing data that are collected and used; the types of viewing data that will be shared with third parties; specific categories of such third parties; and purposes for sharing such information.

Turow Decl. ¶ 32.[8] Professor Turow also concluded that these revised disclosures "are reasonably informative," and "[a]s compared to the previous disclosures, this presentation gives readers a useful overview of what the viewing data collection yields Vizio and possibly them." *Id.* ¶ 28.

Vizio's imposition of prominent and clear disclosures in February 2017, and its shift to an affirmative consent model, is a significant change which resolves a central concern that motivated this lawsuit and the Federal Trade Commission's investigation.

[8] The disclosures negotiated by the parties also address these categories of information. *See id.*

Vizio acknowledges that "Plaintiffs' filing of this Action was a substantial cause of VIZIO's implementation of the Disclosures." Settlement ¶ A.12.

The parties have negotiated further changes to the on-screen disclosure for new customers and have secured an agreement that Vizio will disclose viewing data collection in a "quick-start" guide. Turow Decl. ¶¶ 5, 7, 31-33. The disclosures will be displayed in substantially the same form for the next five years. *Id.* ¶ 5.

The changes to the on-screen disclosure are two-fold. First, a "Decline" button will now appear next to an "Accept" button. *Id.* ¶ 31. The "Decline" button replaces the Settings button and different process for declining data collection, which Professor Turow describes in his declaration. *Id.*

Second, the disclosure now explicitly states that "Declining Viewing Data collection will not change the functionality of your device." *Id.* Disabling viewing data collection on Smart TVs of other manufacturers can change the functionality of the TV, including key features. The language to be added effectively informs consumers of Vizio Smart TVs "that there have not been adverse consequences in terms of functionality if viewing data collection is declined." *Id.*

In addition to the on-screen disclosure, Vizio will include additional language in the device's quick start guide . . . [that] alerts the customer to the right and ability to make a decision during installation about allowing Vizio's viewing data sharing[,] . . . [and] increases the chances that customers will pause and think about what choice is best for them." *Id.*

Professor Turow concludes, based on his evaluation of these disclosures and the disclosures of other manufacturers, "that the result is far superior to the disclosures (or non-disclosures) that prompted this litigation and will be among the best in the industry." *Id.* ¶ 34.. He further writes:

> This court proceeding is to be commended for setting a precedent of significance. Its resolution signals to the industry the importance of obtaining affirmative consent from a consumer before viewing data is collected, and it provides a template for a prominent and clear disclosure that

> allows a consumer to make an informed decision. Equally significant, this precedent is being set at a time when the Smart TV viewing-data collection industry is emerging.

Id. ¶ 8.

The final business practice change we will mention here is Vizio's agreement to delete the remaining contested viewing data in its possession. Under the governmental consent decree, Vizio was obligated to destroy viewing data that was collected prior to March 1, 2016, unless a user of the television subsequently affirmatively consented to viewing data collection when presented with the revised notices.

Under the settlement agreement, Vizio will extend the deletion period to correspond with the class period and will destroy all viewing data collected during the class period without exception. A third party will verify that the viewing data has been successfully destroyed and will report to class counsel. If class counsel does not receive such verification within the time specified by agreement, it is obligated to inform this Court, which retains continuing jurisdiction to address any issues with the enforcement of the settlement agreement.

These changes will take place after the effective date of finality.

D. Release

In exchange for the benefits provided under the settlement, the Plaintiffs and settlement class members will release any legal claims that may arise from or relate to the facts alleged or that could have been alleged in this action. This release is appropriately tailored to the claims litigated to date in this multi-district litigation in that it extends only to the "Vizio Released Parties" and does not include any other individual or entity.

E. Notice

The settlement proposes notice by electronic means.

First, notice will be provided directly to Vizio Smart TVs three separate times, unless a person viewing the notice selects to dismiss the notice, in which case it will only appear one more time (for a total of two times). The notice will time out after 45 seconds. It tells class members that this is a class action; it references the class definition

("Purchased a VIZIO Smart TV Connected to the Internet Between February 1, 2014 and February 6, 2017? You Could Get Money From a $17 Million Class Action Settlement"). And it informs the reader that the class alleges privacy and consumer protection claims; that a class member may appear through an attorney if the member wants; that class members can be excluded; the time and manner for requesting exclusion; and the binding effect of a class judgment. It includes the date by which to file a claim and provides the address for a settlement website, which hosts the Long Form notice and important pleadings and other filings. This notice is estimated to reach 6 million Smart TVs.

Second, a substantially similar notice will also be sent to approximately 9 million potential class members via e-mail. The settlement administrator will use best practices to increase deliverability and verify the number of e-mails successfully delivered

The sample notices do not yet include estimated compensation but an appropriate estimated range for the notices would be $13 to $31, which assumes a 2 percent to 5 percent claims rate.

Third, a digital media campaign will supplement the TV and e-mail notices. As explained further in the Declaration of Eric Schacter of A.B. Data, this campaign will execute digital banners ads through the Google Display Network, Facebook (which includes a settlement-specific Facebook page) and Google AdWords/Search platforms. A minimum of 62 million impressions will be delivered. The campaign will also include a notice through a press release over PR Newswire's US1 and Hispanic Newslines. After the press release is disseminated, both A.B. Data and PR Newswire will post the press release on their respective Twitter pages. A copy of a digital banner ad is attached to the Declaration of Eric Schacter of A.B. Data.

Lastly, the settlement administrator will set up a case-specific webpage for a long form notice in English and Spanish, to host pleadings, to provide case updates, contact information for the settlement administrator, as well as other information. The English version of the long form notice is attached to the settlement agreement as an exhibit.

The notice and notice plan is further described below in Section V.C-D, the

Declaration of Eric Schachter of A.B. Data, and the settlement agreement.

F. Administration

The settlement agreement provides that payment will issue upon finality to class members who submit valid a valid claim form. The claim form is attached to the Declaration of Eric Schacter of A.B. Data, which describes the plan of allocation.

The settlement agreement also provides that the Settlement Administrator shall disseminate the notice and implement the notice. And it provides procedures for exclusion from the settlement class or to comment on or opt out of the settlement class.

Deadlines for these events and also the final approval hearing are proposed as follows, under the assumption that an order granting preliminary approval issues on or soon after December 7, 2018:

Event	Date
Notice of Class Action Settlement completed per Notice Plan	February 26, 2019
Deadline for Class Counsel to File Motion for Final Approval	March 19, 2019
Deadline for Class Counsel to File Motion for Attorney's Fees and Costs	March 19, 2019
Opt-Out and Objection Deadline	April 12, 2019
Reply in Support of Motions for Final Approval and Attorney's Fees and Costs	May 3, 2019
Final Approval Hearing	May 31, 2019

IV. Argument

The procedure for judicial approval of a proposed class action settlement under Rule 23(e) typically involves three main steps:

(1) Certification of a settlement class and preliminary approval of the proposed settlement after submission to the Court of a written motion for preliminary

approval.

(2) Dissemination of notice of the proposed settlement to the class members.

(3) A hearing at which evidence and argument concerning the fairness, adequacy, and reasonableness of the proposed settlement may be presented.

See Federal Judicial Center, Manual for Complex Litigation, Fourth § 21.63 (2004).

Plaintiffs respectfully request that the Court begin this process by provisionally certifying the proposed settlement class, granting preliminary approval of the proposed settlement, and directing that notice be provided.

At the outset, we note that pending before Congress are amendments to Federal Rule of Civil Procedure 23 that have been adopted by the Supreme Court of the United States pursuant to 28 U.S.C. 2072. "Among other things, the amendments require lawyers to provide additional information up front for the court to preliminarily approve settlements ('frontloading'), permit notice by electronic means, impose limitations on compensating objectors, and clarify final-settlement criteria." Bolch Judicial Institute, *Guidelines and Best Practices Implementing 2018 Amendments to Rule 23 Class Action Settlement Provisions*, Duke Law School (August 2018), at *ii.[9]

The amendments will take effect on December 1, 2018, absent action by Congress, and will "govern in all proceedings in civil cases thereafter commenced and, insofar as just and practicable, all proceedings then pending." April 26, 2018 Order of Supreme Court.[10] Because Congress rarely takes such action, we apply here the soon-to-be-amended Rule 23 because this proceeding (and possibly this motion) will be pending when the new rule takes effect in December, and because it is not impracticable or unjust to apply the new rule to this case.

A. Certification of the Proposed Settlement Class Is Appropriate.

The Court should conditionally certify the settlement class for settlement purposes

[9] *Available at* https://judicialstudies.duke.edu/wp-content/uploads/2018/09/Class-Actions-Best-Practices-Final-Version.pdf.

[10] www.supremecourt.gov/orders/courtorders/frcv18_5924.pdf (page 3 of 18). A copy of the amendments to this rule is available at this link.

under Rule 23(a) and 23(b)(3) based on violations of the federal Video Privacy Protection Act, 18 U.S.C. § 2710, and Wiretap Act, *see* 18 U.S.C. § 2520(a).

"When conditionally certifying a class for settlement purposes, the Court 'must pay undiluted, even heightened, attention to class certification requirements.'" *Munday v. Navy Fed. Credit Union*, No. SACV151629-JLS-KESx, 2016 WL 7655807, at *2 (C.D. Cal. Sept. 15, 2016) (citing *Staton v. Boeing Co.*, 327 F.3d 938, 952-53 (9th Cir. 2003) (internal quotation marks omitted). "A party seeking class certification must satisfy the requirements of Federal Rule of Civil Procedure 23(a) and the requirements of at least one of the categories under Rule 23(b)." *Wang v. Chinese Daily News, Inc.*, 737 F.3d 538, 542 (9th Cir. 2013). Rule 23 does not set forth a mere pleading standard," but rather requires the movant to be "prepared to prove that there are in fact sufficiently numerous parties, common questions of law or fact, etc." *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 350 (2011) (emphasis removed). The Court, in turn, must engage in a "rigorous analysis" of Rule 23 criteria, which frequently overlaps with the merits. *Id.* That said, the Court can "consider merits questions at the class certification stage only to the extent they are relevant to whether Rule 23 requirements have been met." *Torres v. Mercer Canyons Inc.*, 835 F.3d 1125, 1133 (9th Cir. 2016).

"Rule 23(a) ensures that the named plaintiffs are appropriate representatives of the class whose claims they wish to litigate." *Dukes*, 564 U.S. at 349. It sets forth four requirements a party seeking class certification must satisfy: numerosity, commonality, typicality, and adequacy. Fed. R. Civ. P. 23(a).

"A proposed class must also satisfy the requirements for at least one of the three types of class actions enumerated in Rule 23(b)." *Munday*, 2016 WL 7655807, at *3. Here, Plaintiffs seek certification under Rule 23(b)(3), which authorizes a class proceeding if "the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy." Fed. R. Civ. P. 23(b)(3).

1. Rule 23(a) Is Satisfied.

a. The Class Members Are Too Numerous to Be Joined.

The proposed class is so numerous that joinder of all members is impracticable. *See* Fed. R. Civ. P. 23(a)(1). Vizio collected viewing data from Smart TVs that were connected to the Internet between February 1, 2014 and February 6, 2017. All such TVs had automated content recognition software installed, including the SmartCast product line.[11] Vizio estimates that 16 million TVs connected to its servers during the settlement class period. Because the class is defined as one purchaser per household per television, numerosity is plainly met.

b. The Action Involves Common Questions of Law or Fact.

Under Rule 23(a)(2)'s requirement that there be "questions of law or fact common to the class," the claims "must depend upon a common contention" such that "determination of [their] truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke." *Dukes*, 564 U.S. at 350. "What matters to class certification . . . is not the raising of common 'questions'—even in droves—but, rather the capacity of a classwide proceeding to generate common answers apt to drive the resolution of the litigation." *Id.* (internal citation omitted, emphasis removed).

Here, commonality is satisfied because the "circumstances of each particular class member . . . retain a common core of factual or legal issues with the rest of the class." *Evon v. Law Offices of Sidney Mickell*, 688 F.3d 1015, 1029 (9th Cir. 2012) (citations and quotations omitted). Plaintiffs' claims center on whether Vizio collected and shared what Plaintiffs consider to be personally identifiable viewing data without consumers' knowledge or consent. Because the core issues of Vizio's nondisclosure and the collection and sharing of viewing data is common to the claims, Plaintiffs have met their "minimal" burden of demonstrating commonality. *See Astiana v. Kashi Co.*, 291 F.R.D. 493, 502 (C.D. Cal. 2013).

[11] Viewing data was not collected from a small percentage of SmartCast TVs during the class period; however, it would be administratively difficult to exclude purchasers of such TVs during the class period.

c. Plaintiffs' Claims Are Typical of Those of the Class.

"[R]epresentative claims are 'typical' [under Rule 23(a)(3)] if they are reasonably coextensive with those of absent class members." *Torres*, 835 F.3d at 1141. "Measures of typicality include 'whether other members have the same or similar injury, whether the action is based on conduct which is not unique to the named plaintiffs, and whether other class members have been injured in the same course of conduct.'" *Id.* (citation omitted).

Here, the claims of Plaintiffs and all class members arise out of the same course of conduct—the alleged collection and sharing of personally identifiable viewing data without consumers' knowledge or consent—and assert the same theories of liability. As a result, the typicality requirement is satisfied.

d. Plaintiffs and Their Counsel Will Fairly and Adequately Protect the Interests of Class Members.

The test for evaluating adequacy of representation under Rule 23(a)(4) is: "(1) Do the representative plaintiffs and their counsel have any conflicts of interest with other class members; and (2) will the representative plaintiffs and their counsel prosecute the action vigorously on behalf of the class?" *Staton*, 327 F.3d at 957.

In this instance, there is no conflict between Plaintiffs and the settlement class members. Plaintiffs were allegedly harmed in the same way as all class members when their personally identifiable viewing data was collected without their consent or knowledge. In light of this common injury, the named Plaintiffs have every incentive to vigorously pursue the class claims. And in fact, each has done so: Plaintiffs have made important contributions to the case, including by preparing and sitting for depositions. Each Plaintiff has agreed to undertake the responsibilities of serving as a class representative, and each has sworn that he or she will continue to act in the class members' best interests.

Class counsel likewise are qualified to continue representing the class. The Court appointed us as interim co-lead class counsel because of our experience in data privacy and consumer class actions. Since then, this Court and Magistrate Judge Scott have had an

opportunity to review class counsel's written work and oral presentations, including the work of Andre Mura and Adam Zapala. The results obtained in the course of litigation and settlement negotiations confirm counsel's adequacy.

2. Rule 23(b)(3) Is Satisfied.

a. Common Questions of Fact and Law Predominate.

Predominance analysis under Rule 23(b)(3) "focuses on the relationship between the common and individual issues in the case, and tests whether the proposed class is sufficiently cohesive . . . ." *Ehret v. Uber Techs., Inc.*, 148 F. Supp. 3d 884, 894-95 (N.D. Cal. 2015) (quoting *Abdullah v. U.S. Sec. Assocs.*, 731 F.3d 952, 964 (9th Cir. 2013)). "When a proposed class challenges a uniform policy, the validity of that policy tends to be the predominant issue in the litigation." *Nicholson v. UTI Worldwide, Inc.*, No. 3:09-cv-722-JPG-DGW, 2011 WL 1775726, at *7 (S.D. Ill. May 10, 2011) (citation omitted). Further, when a settlement class is proposed, the manageability criteria of Rule 23(b)(3) do not apply. *Amchem Prods. v. Windsor*, 521 U.S. 591, 620 (1997).

This case involves an alleged uniform policy of Vizio to equip its Smart TVs with software that collects viewing data to license to third parties, in order to create an additional revenue stream for Vizio. The common thread running through Plaintiffs' federal privacy claims—the Video Privacy Protection Act, and the Wiretap Act—is that Vizio allegedly collected (or intercepted) personally identifiable viewing data, without consumers' consent or knowledge, as this viewing data was communicated on the TV screen.[12] Plaintiffs allege Vizio then licensed this sensitive viewing data to third parties—along with information about their digital identities—thus allegedly enabling these third parties to connect viewing data with individuals on a personal, or household, level.

Because the technology at issue operated uniformly across Vizio's TVs, legal and

[12] This is likewise a core allegation for Plaintiffs' state-law privacy claims. These state laws are closely related to federal privacy law. *See In re Vizio, Inc., Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1215 (C.D. Cal. 2017) ("Plaintiffs' federal claims under the Wiretap Act bear a 'close relationship' to the tort of invasion of privacy."). Also, this allegation addresses issues important to the consumer protection claims, which ask whether Vizio adequately informed consumers of this data collection and licensing.

factual issues respecting collection and disclosure may be resolved for all in a single adjudication. Issues of consent or knowledge may also be answered for all on a class-wide basis, because arguably there is no evidence of any adequate disclosure of the collection of viewing data during the class period. Consequently, central issues common to the class predominate over any individual considerations that might arise.

Finally, because conditional certification of a single nationwide class is based on violations of federal law, there can be no argument that differences in state law defeat predominance.[13] *See Gustafson v. BAC Home Loans Servicing, LP*, 294 F.R.D. 529, 544 (C.D. Cal. 2013); *see also In re Mex. Money Transfer Litig.*, 267 F.3d 743, 747 (7th Cir. 2001) (class representatives can meet the predominance requirement by limiting their legal theories to aspects of law that are uniform).

b. A Class Action Is the Superior Method for Resolving These Claims.

A class action is superior under Rule 23(b)(3) because it represents the only realistic means through which purchasers of affected Smart TVs may obtain relief. *See, e.g., Valentino v. Carter-Wallace, Inc.*, 97 F.3d 1227, 1234 (9th Cir. 1996) (explaining that a class action may be superior where "classwide litigation of common issues will reduce litigation costs and promote greater efficiency"). Even assuming class members could recover statutory damages, they nonetheless would lack an incentive to bring their own cases given the high expert costs involved in litigating a case such as this concerning complex technology. *Mullins v. Premier Nutrition Corp.*, No. 13-CV-01271-RS, 2016 WL 1535057, at

[13] Such an argument would fail on its own terms. "Variations in state law do not necessarily preclude a 23(b)(3) action," and would not do so here if conditional certification of consumer claims were sought, because of "the commonality of substantive law applicable to all class members." *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1022 (9th Cir. 1998); *id.* at 1022-23 (concluding "the idiosyncratic differences between state consumer protection laws are not sufficiently substantive to predominate over the shared claims"); *In re Hyundai And Kia Fuel Econ. Litig.*, 897 F.3d 1003, 1007 (9th Cir. 2018) (granting en banc review of this issue). In any event, here the issue is academic, because conditional certification of a nationwide class is based on federal law, which fully suffices for purposes of preliminary and final approval of this settlement.

*8 (N.D. Cal. Apr. 15, 2016) ("Cases, such as this, 'where litigation costs dwarf potential recovery' are paradigmatic examples of those well-suited for classwide prosecution.") (quoting *Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1023 (9th Cir. 1998)).

3. Appointment of Class Counsel Is Merited.

Under Rule 23(g), "a court that certifies a class must appoint class counsel." Fed. R. Civ. P. 23(g). As discussed above in addressing the adequacy requirement of Rule 23(a), Eric Gibbs and Andre Mura of Gibbs Law Group LLP, and Joseph Cotchett and Adam Zapala of Cotchett, Pitre, McCarthy LLP, each possesses the necessary skill and expertise to ably represent the class, as each has to date. The Court should thus appoint these four lawyers as class counsel.

* * *

For all these reasons, the proposed settlement class merits provisional certification.

B. Preliminary Approval of the Settlement Is Warranted.

"To preliminarily approve a proposed class action settlement, Rule 23(e)(2) requires the Court to determine whether the proposed settlement is fair, reasonable, and adequate." *Oda v. DeMarini Sports, Inc.*, No. 8:15-cv-2131-JLS-JCGx, slip op. at 13 (C.D. Cal. June 6, 2018) (Doc. 157) (citing Fed. R. Civ. P. 23(e)(2)). If preliminary approval is granted, the Court will examine many of the same procedural and substantive factors at the approval stage that it is now considering at this notice stage. *Id.*

"A proposed settlement that is 'fair, adequate and free from collusion' will pass judicial muster."'*In re Volkswagen "Clean Diesel" Mktg., Sales Practices, & Prod. Liab. Litig.*, 895 F.3d 597, 610 (9th Cir. 2018). "To determine whether a settlement agreement meets these standards, a district court must consider a number of factors, including: the strength of plaintiffs' case; the risk, expense, complexity, and likely duration of further litigation; the risk of maintaining class action status throughout the trial; the amount offered in settlement; the extent of discovery completed, and the stage of the proceedings; the experience and views of counsel; the presence of a governmental participant; and the reaction of the class members to the proposed settlement." *Staton*, 327 F.3d at 959

(internal citation and quotation marks omitted).

In addition, "[w]hen, as here, the settlement was negotiated before the district court certified the class, 'there is an even greater potential for a breach of fiduciary duty' by class counsel, so we require the district court to undertake an additional search for 'more subtle signs that class counsel have allowed pursuit of their own self-interests and that of certain class members to infect the negotiations.'" *In re Volkswagen*, 895 F.3d at 610–11. "Such signs include (1) when counsel receive a disproportionate distribution of the settlement, (2) when the parties negotiate a clear sailing arrangement providing for the payment of attorneys' fees separate and apart from class funds, and (3) when the parties arrange for fees not awarded to revert to defendants rather than be added to the class fund." *Oda*, No. 8:15-cv-2131-JLS-JCGx, slip op. at 14 (citing *In re Bluetooth Headset Prod. Liab. Litig.*, 654 F.3d 935, 946-47 (9th Cir. 2011)).

The 2018 amendments to Rule 23(e) similarly require counsel to provide additional information up front at the preliminary approval stage, so that the court can determine whether it "will likely be able to [finally] approve" it. Duke Law School, *Implementing 2018 Amendments to Rule 23*, *supra*, at *2. This information must address the adequacy of class representatives and class counsel; whether the settlement proposal was negotiated at arm's length; the relief provided to the class, in view of a variety of factors, including the costs, risks, and delay of trial and appeal; the effectiveness of any proposed method of distributing relief to the class, including the method of processing class-member claims; the terms of any proposed award of attorney's fees, including timing of payment; and any agreement required to be identified under Rule 23(e)(3); and lastly whether the proposal treats class members equitably relative to each other.

Ultimately, however, the factors are "guideposts. 'The relative degree of importance to be attached to any particular factor will depend upon . . . the unique facts and circumstances presented by each individual case.'" *In re Volkswagen*, 895 F.3d at 611 (citing *Officers for Justice v. Civil Serv. Comm'n of City & Cnty. of San Francisco*, 688 F.2d 615, 625 (9th Cir. 1982). "Deciding whether a settlement is fair is ultimately an amalgam of delicate

balancing, gross approximations and rough justice," that is "best left" to the sound discretion of the trial judge. *Id.* (internal citation and quotation marks omitted).

Furthermore, "[a]t this preliminary stage and because Class Members will receive an opportunity to be heard on the Settlement Agreement, a full fairness analysis is unnecessary." *Oda*, No. 8:15-cv-2131-JLS-JCGx, slip op. at 14 (citation and quotation marks omitted). The 2018 amendments to Rule 23 do not change this law. Despite requiring courts to ask whether a proposed settlement is likely to win final approval, the preliminary approval standard remains "more lenient than the eventual standard required to grant final approval." Duke Law School, *Implementing 2018 Amendments to Rule 23*, *supra*, at *2.

As such, "preliminary approval and notice of the settlement terms to the proposed Class are appropriate where '[1] the proposed settlement appears to be the product of serious, informed, non-collusive negotiations, [2] has no obvious deficiencies, [3] does not improperly grant preferential treatment to class representatives or segments of the class, and [4] falls within the range of *possible* approval . . . .'" *Oda*, No. 8:15-cv-2131-JLS-JCGx, slip op. at 15 (citing *In re Tableware Antitrust Litig.*, 484 F. Supp. 2d 1078, 1079 (N.D. Cal. 2007) (emphasis supplied by *Oda*); *see also Acosta v. Trans Union*, LLC, 243 F.R.D. 377, 386 (C.D. Cal. 2007) ("To determine whether preliminary approval is appropriate, the settlement need only be *potentially* fair, as the Court will make a final determination of its adequacy at the hearing on the Final Approval, after such time as any party has had a chance to object and/or opt out.") (emphasis in original).

After evaluating the "lengthy but non-exhaustive list of [overlapping fairness] factors," *In re Volkswagen*, 895 F.3d at 610, the Court should preliminarily approve the settlement agreement because it is fair, reasonable, and adequate, and will likely be granted final approval.

1. Strength of Plaintiffs' Case

As mentioned, the principal claims at issue here involve Vizio's alleged collection and licensing of viewing data without consumers' knowledge or consent. The collection of

the content of this communication in real time (Wiretap Act) for purposes of licensing to third parties (VPPA) without consumers' knowledge or consent (Wiretap, VPPA) are core issues that unite Plaintiffs' federal privacy claims, and are similarly critical to the resolution of Plaintiffs' state-law privacy claims (the scope of the intrusion and the sensitivity of the information obtained) and consumer-protection claims (whether these practices were adequately disclosed in marketing materials or privacy policies). If these legal theories were proven at summary judgment or trial, Plaintiffs could theoretically be entitled to liquidated or statutory damages under the VPPA or Wiretap Act, for $2,500 and $10,000, respectively.[14]

Plaintiffs allege that the viewing data is sensitive and personally identifies them. Vizio disputes the sensitive and personal nature of the data collected and shared. The recent decision in *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 981 (9th Cir. 2017), throws a wrench in the gears of Plaintiffs' case. There, the Ninth Circuit held that "personally identifiable information" under the VPPA includes only information that readily permits an ordinary person to identify a particular individual as having watched certain videos. *Id.* at 985. This is a less forgiving legal standard than that applied by the First Circuit in *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016), and adopted by this Court: "whether a video tape service provider can escape liability for disclosures that would reasonably and foreseeably result in identifying a specific person as watching a particular program merely because an 'ordinary person' would not be able, on her own, to identify the consumer." Order Denying Mot. for Interlocutory Appeal, Doc 224 at 12

[14] For almost the entire class period, the California wiretap act authorized a single $5,000 award of statutory damages per individual, rather than an award per violation. *See Ramos v. Capital One, N.A.*, No. 17-CV-00435-BLF, 2017 WL 3232488, at *5-7 (N.D. Cal. July 27, 2017), *appeal dismissed*, No. 17-16723, 2017 WL 5891737 (9th Cir. Nov. 14, 2017). Still, because the elements of the federal and state wiretap claims are essentially the same, and because these two laws arguably serve the same remedial purpose, courts applying California law might not allow a California plaintiff to recover multiple statutory penalties for the same wiretap. *See Los Angeles Cnty. Metro. Transp. Auth. v. Superior Court*, 123 Cal. App. 4th 261, 267 (2004). We thus consider the federal Wiretap Act claim only, though it hardly matters whether we consider only one wiretap act or both; either way, any such award of statutory damages would be colossal and could never be recovered from Vizio.

n.4.[15]

Applied here, *Eichenberger*'s more restrictive standard for "personally identifiable information" under the VPPA would be difficult to meet. Put simply, whether the information Vizio discloses would require too much detective work for an ordinary person to link an individual to viewing data is a factual matter that could be challenging for Plaintiffs to establish under Ninth Circuit law. We say this recognizing that the Ninth Circuit itself left the open the possibility that "modern technology may indeed alter—or may already have altered—what qualifies under the statute" as personally identifiable. 876 F.3d at 986.

The Wiretap Act claim also raises issues of first impression in this circuit. The statute authorizes "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter" to sue for damages. 18 U.S.C. § 2520(a). Vizio has argued that it does not "intercept" any electronic communications, and the messages it collects do not constitute the "contents" of an electronic communication. Plaintiffs, in turn, believe there is favorable evidence supporting the real-time nature of the interception of the contents of a communication.

Even so, whether information qualifies as having been "intercepted" within the meaning of the Wiretap Act, if it is acquired simultaneously with its arrival on the Smart TV, has not been established. The Ninth Circuit in *Konop v. Hawaiian Airlines* suggested in dicta that the Wiretap Act might not be implicated by such facts, but it did not resolve the issue. 302 F.3d 868, 878 (9th Cir. 2002).

This Court identified legal authority to support the view that such an acquisition "satisfies the contemporaneous interception requirement." *In re Vizio*, 238 F. Supp. 3d at

[15] While *Yershov* sets forth a more forgiving legal standard, it was nonetheless insurmountable in that case. *See Yershov*, Joint Stipulation of Dismissal With Prejudice, Case No. 1:14-cv-13112-FDS (D. Mass. March 27, 2017) (Doc. 83 at 1) ("the Parties agree that Plaintiff lacks sufficient evidence to support his allegation that Defendant violated the Video Privacy Protection Act by 'disclosing his PII—in the form of the title of the videos he watched [on the USA Today App], his unique Android ID, and his GPS coordinates—to third party analytics company Adobe Systems Inc.' from which Adobe identified Yershov and attributed his video viewing records to an individualized profile of Plaintiff Yershov in its databases.") (brackets and internal quotation marks removed).

1226 (citing *United States v. Szymuszkiewicz*, 622 F.3d 701, 706 (7th Cir. 2010)). Plaintiffs would defend that view. But *Szymuszkiewicz* has been criticized by a leading Fourth Amendment scholar who claims the Seventh Circuit misread the Wiretap Act. Orin Kerr, *The Perils of Interpreting Statutes With Multiple Remedial Schemes: A Comment on the Dicta in United States v. Szymuszkiewicz*, The Volokh Conspiracy blog.[16] The professor's arguments have some force, so it is not free from doubt that Plaintiffs could prevail on their Wiretap Act claim.[17]

As for Plaintiffs' remaining claims, their strength on the merits may largely turn on whether consumers were adequately advised that their viewing data would be collected and shared. The parties disagree on this point, because Plaintiffs believe there is evidence that Vizio's disclosures in marketing materials and privacy policies during the class period were inadequate.

In addition, the remaining claims may turn on whether the information collected is deemed sensitive. This matters both for purposes of materiality under the consumer-protection claims and the state privacy claims, which may be actionable when community norms are violated. Again, the parties disagree on the degree of risk for these claims. If the named Plaintiffs' negative reaction to Vizio's conduct is any indication, however, likeminded jurors could resolve these factual questions favorably for Plaintiffs.

Finally, even if Plaintiffs are able to establish that Vizio violated these federal privacy laws, "statutory damages are not to be awarded mechanically." *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 268 (N.D. Cal. 2016). The Wiretap Act, for instance, "makes the decision of whether or not to award damages subject to the court's discretion." *DirecTV, Inc. v. Huynh*, 2005 WL 5864467, at *8 (N.D.Cal. May 31, 2005), *aff'd*, 503 F.3d 847 (9th Cir. 2007). This is apparent in the text of the Wiretap Act, "which was amended in 1986

[16] http://volokh.com/2010/09/10/the-perils-of-interpreting-statutes-with-multiple-remedial-schemes-a-comment-on-the-dicta-in-united-states-v-szymuszkiewicz/.

[17] Citing *In re Zynga Privacy Litigation*, 750 F.3d 1098, 1106 (9th Cir. 2014), Vizio has argued that Wiretap Act claim should fail because the information Vizio collects from Smart TVs does not constitute the "contents" of an electronic communication. Plaintiffs disagree with Vizio's reading of *In re Zynga*.

to state that the court 'may' award damages, rather than stating that it 'shall' award damages." *Campbell*, 315 F.R.D. at 268. The Court's "discretion is limited to deciding whether to 'either award the statutory sum or nothing at all,' it 'may not award any amount between those two figures.'" *Id.* (quoting *Huynh*, 2005 WL 5864467, at *8).[18]

In authorizing liquidated damages under the VPPA, Congress employed similar language—"The court may award . . . actual damages but not less than liquidated damages in an amount of $2,500," or punitive damages, 18 U.S.C. § 2710(c)(2)—rather than directing that a court "shall" award such damages. *See id.*

When exercising such discretion, courts consider "(1) whether the defendant profited from his violation; (2) whether there was any evidence that the defendant actually used his pirate access devices; (3) the extent of [plaintiff's] financial harm; (4) the extent of the defendant's violation; (5) whether the defendant had a legitimate reason for his actions; (6) whether an award of damages would serve a legitimate purpose; and (7) whether the defendant was also subject to another judgment based on the same conduct." *Huynh*, 2005 WL 5864467 at *8.[19] If this Court were to conclude that some or many class members suffered little monetary harm from the collection and disclosure of viewing data, it could conclude that any liquidated, statutory, or punitive damages would disproportionately penalize Vizio.[20]

For all these reasons, while aspects of Plaintiffs' claims are strong, Plaintiffs may face considerable headwinds in seeking to establish new law in these complex areas and to

[18] The $10,000 lump sum for liquidated damages is limited to a single award per victim as long as the violations are "interrelated and time compacted." *Smoot v. United Transp. Union*, 246 F.3d 633, 642-645 (6th Cir. 2001).

[19] We see no sensible reason why such factors would not also be germane to the VPPA.

[20] In *Campbell*, the court declined to certify a Rule 23(b)(3) litigation class because it concluded that "sorting out those disproportionate damages awards would require individualized analyses that would predominate over common ones." 315 F.R.D. at 269. Plaintiffs believe this analysis of predominance clashes with *Tyson Foods, Inc. v. Bouaphakeo*, which recognized: "When one or more of the central issues in the action are common to the class and can be said to predominate, the action may be considered proper under Rule 23(b)(3) even though other important matters will have to be tried separately, such as damages or some affirmative defenses peculiar to some individual class members." 136 S. Ct. 1036, 1045 (2016) (internal quotation marks and citation omitted). Therefore, Plaintiffs have not mentioned this case as posing a risk to class certification.

recover more in the way of monetary relief. *See also* Section IV.B.2 (explaining that further litigation could extinguish Plaintiffs' legal entitlement to, and ability to negotiate for, injunctive relief). Overall, then, this factor weighs in favor of preliminary approval.

2. Risk, Complexity, Costs, and Likely Duration of Further Litigation, and Risk of Maintaining Class Certification

This litigation is complex because it "involves several intricate technologies"; it is risky because it requires Plaintiffs to establish new law; and it is expensive because it requires intensive work by qualified experts familiar with the data industry, tracking software, and privacy practices in the digital sphere. Order Denying Mot. for Interlocutory Appeal, Doc. 224 at 5. Neither party is likely to accept a dispositive, adverse ruling without an appeal. The litigation has been intensive to date, and would only become more so, and increasingly costly, if litigation were to continue.

More critically, if this settlement is not approved, it is unlikely that further litigation would lead to a better settlement. This is evident for two reasons. One, there is the risk that Vizio will again seek to limit Plaintiffs' injunctive relief based on its compliance with the consent decree with the Federal Trade Commission. The Court previously denied such a request by Vizio—an important ruling which allowed Plaintiffs to negotiate the injunctive relief in this case. But it did so without prejudice, noting Vizio could yet satisfy its "formidable burden" of demonstrating that "subsequent events make it absolutely clear that the allegedly wrongful behavior could not reasonably be expected to recur." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 189 (2000) (citation omitted).

Two, if Plaintiffs were to succeed in certifying a litigation class, Vizio would then press the Court to "definitively adjudicate the enforceability of the arbitration agreement." Order Denying Mot. to Dismiss and Strike. The arbitration agreement that applies to such class members does not, by its terms, permit class proceedings, and it does not allow the arbitrator to award equitable relief. *See* Brinkman Decl., Exs. A-B, Docs. 142-3, 142-4. Also, monetary relief in arbitration may be limited to actual damages. *Id.*

If either of these two events were to occur, Plaintiffs would be diminished in their ability to negotiate settlement terms as favorable as those in the proposed settlement.

Costs will increase substantially if the litigation continues through class certification, *Daubert* motions, summary judgment, trial, and appeals. Expert costs in particular would be high. Plaintiffs have been judicious in their use of experts to date, but class certification and trial will require considerable work by experts.

Plaintiffs do not see serious obstacles to obtaining and maintaining class certification. Even so, Vizio would vigorously resist class certification, before this Court and on appeal. Even a "small" risk that class certification is not achievable "weigh(s) in favor of granting final approval, as the settlement would eliminate the risk." *Vandervort v. Balboa Capital Corp.*, 8 F. Supp. 3d 1200, 1206 (C.D. Cal. 2014).

This settlement, by comparison, "eliminates the risks inherent in certifying a class, prevailing at trial, and withstanding any subsequent appeals, and it may provide the last opportunity for class members to obtain" monetary and injunctive relief. *Oda*, No. 8:15-cv-2131-JLS-JCGx, slip op. at 16. This factor therefore weights in favor of settlement approval. *See Nat'l Rural Telecomms. Coop. v. DIRECTV, Inc.*, 221 F.R.D. 523, 526 (C.D. Cal. 2004) ("In most situations, unless the settlement is clearly inadequate, its acceptance and approval are preferable to lengthy and expensive litigation with uncertain results." (citation omitted)).

3. Amount Offered in Settlement

"To determine whether a settlement 'falls within the range of possible approval,' courts focus on 'substantive fairness and adequacy' and 'consider plaintiffs' expected recovery balanced against the value of the settlement offer.'" *Schuchard v. Law Office of Rory W. Clark*, No. 15-cv-01329-JSC, 2016 WL 232435, at *10 (N.D. Cal. Jan. 20, 2016) (quoting *Tableware*, 484 F. Supp. 2d at 1080). "Immediate receipt of money through settlement, even if lower than what could potentially be achieved through ultimate success on the merits, has value to a class, especially when compared to risky and costly continued litigation." *In re LinkedIn User Privacy Litig.*, 309 F.R.D. 573, 587 (N.D. Cal. 2015).

The class benefits offered in this settlement—both monetary and injunctive relief—represent an excellent outcome for the class. To begin, the settlement establishes a cash fund of $17,000,000. This is more than the revenue Vizio obtained from licensing viewing data during the class period. *See* Siu Decl. ¶ 11. Plaintiffs' expert calculates that actual harm per consumer is in the range of $0.78 and $4.76. *See* Egelman Rep. at 12. There are approximately 16 million class members. After payment of notice and administration costs and any approved award of attorneys' fees, costs, and service awards, all funds remaining in the settlement fund will be distributed to the class (*i.e.*, "the net settlement fund").

In addition to the monetary benefits obtained through the settlement, Plaintiffs have obtained extensive injunctive relief. Plaintiffs' expert has opined that the value of the injunctive relief is, conservatively, $6 to $8 million. *See* Egelman Rep. at 3, 12. Thus, even assuming that 100 percent of the class submits a claim for payment from the Settlement Fund, each member of the class would theoretically receive up to $0.62 in direct compensation (assuming $10,000,000 in a Net Settlement Fund made available to 16 million class members), plus the value of injunctive relief per class member, which is approximately $0.50. Thus, in a scenario where 100 percent of the class make claims, each class member would receive $1.12 in settlement benefits, which is above 100 percent of the damages a class member could expect to receive at trial at the lower bounded range of the maximum amount recoverable. Assuming a more realistic claims rate of 5 percent—which is still considered on the high end of claims rates for consumer class actions—Plaintiffs estimate that the per class member recovery would be $13.00 ($12.50 from the settlement fund and $0.50 in injunctive relief). These amounts greatly exceed the maximum value of actual harm per consumer, per TV.

Because Plaintiffs' expert estimates that average damages for actual harm from the collection and sharing of viewing data is between $0.78 and $4.76, the ranges that class counsel anticipate as direct payment to class members represents a highly favorable recovery on a per-TV basis. *See* Egelman Rep. at 12. And it is more favorable still once the

value of injunctive relief is considered, as it must be. *Cf. Lee v. Enter. Leasing Co.-W.*, No. 3:10-CV-00326-LRH, 2015 WL 2345540, at *5 n.5 (D. Nev. May 15, 2015) ("[T]he Ninth Circuit considers the value available to the class in determining total value, rather than merely the amount redeemed.") (emphasis removed).

An examination of settlements in similar consumer privacy cases, where parties pleaded claims for statutory damages under the VPPA or Wiretap Act, further confirms the reasonableness of the proposed settlement in this case. *Perkins v LinkedIn*, which concerned the collection and dissemination of user e-mails and address book contents, settled for $13 million. No. 5:13-cv-04303-LHK (N.D. Cal.), Doc. 134 at 4. *Google Referrer Header Privacy Litigation*, which concerned the collection and use of users' search terms, settled for $8.5 million. No. 5:10-cv-04809-EJD (N.D. Cal.), Doc. 85 at 10, *aff'd*, 869 F.3d 737 (2017), *cert. granted*, 138 S. Ct. 1697 (2018). *Sony Gaming Networks*, which concerned the disclosure of Sony PlayStation account holder information, settled for $15 million. No. 3:11-md-02258 (S.D. Cal.), Doc. 204-1 at 6-10. *In re Netflix Privacy Litigation*, which concerned the collection and retention of users' viewing and personal information, settled for $9 million plus injunctive relief valued at $4.65 million. No. 5:11-cv-00379 (N.D. Cal.), Doc. 256 at 10. *Fraley v. Facebook*, which concerned the collection of names and likenesses for promotional purposes, settled for $20 million. No. 3:11-cv-01726 (N.D. Cal.), Doc. 359 at 5. And *Lane v. Facebook*, which concerned the public dissemination of information about members' online activities, settled for $9.5 million. No. 5:08-cv-03845 (N.D. Cal.), Doc. 108 at 4.

Several of the settlements just mentioned—*In re Netflix*, *Google Referrer Header*, and *Lane*—resolved the claims of significantly larger classes. The amounts achieved in those settlements were so small per class member that courts concluded compensation could not feasibly be distributed to class members, and thus directed funds to *cy pres* recipients. This fact further confirms the reasonableness of the settlement benefits achieved in this case.

The reasonableness of the settlement is further supported by the Declaration of

Wilda Siu, senior director of accounting at Vizio, Inc. In this declaration, Ms. Siu discusses Vizio's financial position in relation to the settlement amount, and she confirms the revenue received during the class period from the licensing of viewing data. This evidentiary submission demonstrates that "the aggregate size of the settlement—and, relatedly, each individual claimant's recovery—is fully supported by the reality of Defendants' financial position." *Etter v. Thetford Corp.*, NO. SACV 13-00081-JLS (RNBx), slip op. at 20 (C.D. Cal. Mar. 29, 2016) (Doc. 468) (order granting plaintiffs' renewed motion for preliminary approval of class action settlement).

Finally, the amount of the settlement is fair in view of the claims released by Plaintiffs and the class. Each class member will release claims that were or could have been asserted in this action, and the release does not extend beyond the Vizio released parties. Settlement § XVII.1. Because the release mirrors those that have won approval in other similar cases, its scope supports the conclusion that the amount offered in this settlement is fair. *See Hesse v. Sprint Corp.*, 598 F.3d 581, 590 (9th Cir. 2010) ("A settlement agreement may preclude a party from bringing a related claim in the future even though the claim was not presented and might not have been presentable in the class action, but only where the released claim is based on the identical factual predicate as that underlying the claims in the settled class action." (internal quotation marks and citation omitted)).

4. Method of Distributing Relief

The 2018 amendments to Rule 23 instruct that the effectiveness of any proposed method of distributing relief to the class, including the method of processing class-member claims, should be considered as part of the fairness inquiry. This factor supports approval for several reasons.

For one, A.B. Data will distribute relief directly from the settlement fund to all settlement class members who submit valid claims. The settlement class will have the option to receive payment immediately through electronic payment systems (such as PayPal) or by printed check.

For another, the claims process is not unduly demanding, burdensome, or

oppressive. A claimant need not submit a receipt but must state under oath that he or she is a class member based on the objective criteria set forth in the class definition. *See* Schachter Decl. ¶ 17.

Further, the claims process facilitates the filing of claims. Claimants can complete a claim form on a website or on a paper form, and the case-specific website answers frequently asked questions through a long-form notice and provides a toll-free telephone number with an automated interactive voice response system.

Finally, the claims process will also deter unjustified claims and has appropriate security for electronic payment methods. The e-mail notice will provide a unique pin that is associated with an e-mail address. A.B. Data also employs fraud-detection techniques. The electronic payment walls, in turn, are operated by the payment systems themselves, such as PayPal, and thus have advanced security in place. The class member is simply directed to the platforms of these systems. A.B. Data does not receive any log in or password information.

For all these reasons, the method of distributing relief is reasonable and supports preliminary approval.

5. Attorneys' Fees and Costs, and Service Awards

At this stage, courts do not formally consider whether to approve attorneys' fees or service payments for named Plaintiffs. Nevertheless, in light of the amendments to Rule 23, we forecast the application for such payments.

In the Ninth Circuit, when the percentage-of-recovery method is employed, 25 percent of a common fund is a presumptively reasonable amount of attorneys' fees. *See In re Bluetooth*, 654 F.3d at 942. Here, counsel will not ask for more than 25 percent of the total value of the settlement for monetary *and* injunctive relief. *See Staton*, 327 F.3d at 974 ("where the value to individual class members of benefits deriving from injunctive relief can be accurately ascertained [ ] courts [may] include such relief as part of the value of a common fund for purposes of applying the percentage method of determining fees.").

Plaintiffs will seek service awards of $5,000. This enhancement is set at the Ninth

Circuit's benchmark award for representative plaintiffs. *See In re Online DVD-Rental Antitrust Litig.*, 779 F.3d 934, 947-48 (9th Cir. 2015). It is an appropriate enhancement in this case because the representative Plaintiffs actively participated in the litigation and sat for depositions, and because the cumulative awards sought will constitute a small fraction (0.18 percent) of the total settlement fund. *Rhom v. Thumbtack, Inc.*, No. 16-CV-02008-HSG, 2017 WL 4642409, at *8 (N.D. Cal. Oct. 17, 2017) ("A $5,000 award also equals approximately 1–2% of the total settlement fund, which is consistent with other court-approved enhancements.").

6. Stage of the Proceedings and Extent of Discovery Completed

In order to settle a class action, the parties must have "sufficient information to make an informed decision about settlement." *Linney v. Cellular Alaska P'ship*, 151 F.3d 1234, 1239 (9th Cir. 1998). This information can be obtained through formal or informal discovery. *See Clesceri v. Beach City Investigations & Protective Servs., Inc.*, No. CV-10-3873-JLS (RZx), 2011 WL 320998, at *9 (C.D. Cal. Jan. 27, 2011).

Plaintiffs have engaged in extensive discovery, formally and informally, including the production and review of voluminous documents, interrogatories, depositions of all of the Plaintiffs, and one non-party deposition. Further, Plaintiffs took three Fed. R. Civ P. 30(b)(6) depositions of Vizio and served additional interrogatories in the course of crafting injunctive relief. During this period, Vizio also shared information memorializing business-practice changes that Vizio had made pursuant to its consent decree with the government. The report was provided to Plaintiffs under Fed. R. Evid. 408.

Plaintiffs consulted with leading technologists and privacy experts about the strengths and weaknesses of this case. What's more, Plaintiffs' legal theories were put to adversarial testing through two motions to dismiss, a motion for interlocutory appeal, and numerous discovery motions before Magistrate Judge Scott.

Although the parties are proposing to settle before class certification, they possess sufficient information to make an informed decision about the settlement. This factor, then, weighs in favor of granting preliminary approval.

7. Support of Experienced Counsel

"The recommendations of plaintiffs' counsel should be given a presumption of reasonableness." *In re Omnivision Techs., Inc.*, 559 F. Supp. 2d 1036, 1043 (N.D. Cal. 2008) (citation omitted). In fact, experienced counsel's judgment in this respect carries considerable weight. *See Nat'l Rural Telcoms. Coop. v. DIRECTV, Inc.*, 221 F.R.D. 523, 528 (C.D. Cal. 2004) ("'Great weight' is accorded to the recommendation of counsel, who are most closely acquainted with the facts of the underlying litigation.") (citation omitted).

Class counsel wholeheartedly endorse the settlement agreement as fair, reasonable, and adequate. That endorsement is the product of arm's length negotiations before a former federal judge and following relevant discovery. The Court should therefore credit counsel's recommendation that the settlement warrants preliminary approval. *See Linney v. Cellular Alaska P'ship*, Nos. C-96-3008 DLJ, 1997 WL 450064, at *5 (N.D. Cal. July 18, 1997), *aff'd*, 151 F.3d 1234 (9th Cir. 1998) ("The involvement of experienced class action counsel and the fact that the settlement agreement was reached in arm's length negotiations, after relevant discovery had taken place create a presumption that the agreement is fair.").

8. Positive Views of Class Members

The named Plaintiffs have all submitted declarations summarizing their individual views of the settlement. *See* Hodges Decl., Zufolo Decl., Walsh Decl., Rizzitello Decl., Thomson Decl., and Queenan Decl. All are excited by the benefits achieved for the class and support settlement approval. As the views of other class members are known, the Court may take them into account as well. At this stage, however, all indications are that the class is reacting positively to the proposed settlement.

9. No Signs of Collusion

When, as here, a class settlement is reached before class certification, courts are "particularly vigilant" in searching for signs of collusion. *In re Bluetooth*, 654 F.3d at 946–47. Courts must look for explicit collusion and "more subtle signs that class counsel have allowed pursuit of their own self-interests and that of certain class members to infect the

negotiations." *Id.* at 947. Such signs include "when the parties arrange for fees not awarded to revert to defendants rather than be added to the class fund," disproportionate distributions of settlement funds to counsel, and clear-sailing arrangements. *Id.*

There are no signs, explicit or subtle, of collusion between the parties here. First, settlement funds will not revert to Vizio under any circumstances. Settlement funds will go to class members, and the use of electronic payment methods will increase the chances that even small dollar amounts can be distributed to the class. These payments will be divided proportionally among purchasers per TV per household, and thus all class members are treated equitably. The same may be said for the injunctive relief which admits no distinctions among class members. The named Plaintiffs, moreover, have stated under oath that they understand they are not legally entitled to any benefits other than those available to all settlement class members.

Any amount that is not feasibly distributable to the class will be split by next-best recipients. Plaintiffs propose that the next-best recipients should be: Electronic Privacy Information Center, Privacy Rights Clearinghouse, and World Privacy Forum. Any residual would be divided evenly. These organizations submitted applications in which they explained how they would commit to use distributed funds in a specified way that benefits the class or substantial portions of it and addresses issues related to the basis of the lawsuit. And each was asked to confirm that the organization is independent of the parties, their counsel, and the district court. The applications which Plaintiffs received are being submitted to the Court so that it can independently determine the suitability of these next-best recipients. *See* Joint Decl., Ex. 4. This process further confirms that there is no collusion.

Second, there will not be a disproportionate distribution of the settlement fund to counsel.

Third, under the settlement agreement, attorneys' fees are to be awarded from the settlement fund. Although Vizio informed Plaintiffs, after all material class settlement benefits had been negotiated, that it would not oppose an application for fees that does

not exceed 33% of $17,000,000, the settlement agreement explicitly says that the Court is to determine the proportion of the settlement fund that will be awarded as attorneys' fees. Thus, the agreement does not in any way affect the Court's "supervisory discretion" in approving fees. *See Vandervort v. Balboa Capital Corp.*, 2013 WL 12123234, at *5 (C.D. Cal. Nov. 20, 2013) (quoting *Staton*, 327 F.3d at 970).

The timing of the payment of attorneys' fees—shortly after the final approval of fees by this Court—is not controversial, either. *Pelzer v. Vassalle*, 655 Fed. App'x 352, 365 (6th Cir. 2016) ("Quick-pay provisions are common.") (citing Brian T. Fitzpatrick, *The End of Objector Blackmail?*, 62 Vand. L. Rev. 1623, 1643 (2009), which found over one-third of federal class action settlement agreements in 2006 included quick-pay provisions); *Brown v. Hain Celestial Group, Inc.,* 2016 WL 631880, at *10 (N.D. Cal. Feb. 17, 2016) ("Courts . . . approve these 'quick pay' provisions routinely.") (citation omitted); *In re TFT-LCD (Flat Panel) Antitrust Litig.*, 2011 WL 7575004, at *1 (N.D. Cal. Dec. 27, 2011) (same).

Lastly, there is no undisclosed agreement made in connection with the settlement proposal.

For all these reasons, there is no cause for concern that the settlement is the product of collusion.

* * *

Considering all these guideposts, the Court should preliminarily conclude that the proposed settlement is fair, reasonable, and adequate, and likely to receive final approval.

C. Approval of the Proposed Settlement Administrator

Plaintiffs propose, and Vizio does not oppose, the appointment of A.B. Data, Ltd. as settlement administrator. Documentation of A.B. Data's competence is included in the Declaration of Eric Schacter, vice-president of this company. Notably, this Court has previously approved of A.B. Data as a settlement administrator in another class action settlement. *Munday v. Navy Federal Credit Union*, 2016 WL 7655796, at *9 (C.D. Cal. Sep. 15, 2016) (Staton., J.) (order granting renewed joint motion for preliminary approval of class action settlement). For these reasons, the Court should appoint A.B. Data to serve in this

capacity in this case.[21]

D. Preliminary Approval of Class Notice Form and Method

Even as amended in 2018, Fed. R. Civ. P. 23(c)(b)(2) requires the "best notice that is practicable under the circumstances, including individual notice to all members who can be identified through reasonable effort" for certified (b)(3) litigation classes. S. Ct., *Proposed Amendments to the Fed. R. Civ. P.*, at *6.[22] The 2018 amendments apply the requirements of subdivision (c)(2)(B) to the notice of class-action settlements for (b)(3) classes. The settlement agreement contemplates a single, combined notice advising the class of the proposed certification and settlement of (b)(3) classes under both Rule 23(e)(1) and (c)(2)(B).

Rule 23(c)(2)(B) was amended because means of communication have evolved and permitting notice by *electronic* means, including e-mails, digital media, and social media, may provide the best practicable notice under the circumstances. Duke Law School, *Implementing 2018 Amendments to Rule 23*, *supra*, Rules Appendix C, at *17-18.[23] Specifically, the amended language expressly provides that notice can be made by one or a combination of means, including "United States mail, electronic means, or other appropriate means." *See* S. Ct., *Proposed Amendments*, *supra,* at *6.

The Committee Note to amended Rule 23 advises: "Counsel should consider which method or methods of giving notice will be most effective; simply assuming that the 'traditional' methods are best may disregard contemporary communication realities." Duke Law School, *Implementing 2018 Amendments to Rule 23, supra*, Rules Appendix C, at *19. Consistent with that directive, counsel for the parties and the settlement administrator have carefully considered cost, customer preference, and effectiveness, in determining the best practicable means of communicating the settlement benefits and

[21] Plaintiffs will apply for an award of costs to A.B. Data for settlement administration concurrently with their application for attorneys' fees and service payments.

[22] *Available at* https://www.fjc.gov/sites/default/files/materials/58/frcv18_5924.pdf.

[23] *Available at* https://judicialstudies.duke.edu/wp-content/uploads/2018/09/Class-Actions-Best-Practices-Final-Version.pdf.

rights of exclusion (among other matters) to the class.

Vizio has communicated with its customers directly through affected TVs to provide disclosures during and after the class period. Working with the settlement administrator, the parties and the Court will know precisely the number of affected Smart TVs which successfully display the on-screen notice.

The parties have a solid sense of the number of Smart TVs capable of displaying the notice based upon the number of TVs which have communicated with Vizio's servers within the last 3 months and 6 months. Based on these estimates, notice will be sent through the Internet directly to approximately 6,000,000 Vizio TVs purchased by potential Settlement Class Members. As such, the notice will effectively reach the class.

The notice will display three times for 45 seconds, unless the option to dismiss the notice is selected, in which case it will display a second time but not a third time. The easy-to-remember settlement website address—www.VizioTVsettlement.com—is displayed prominently in the center of the screen and in large font. Because of the frequency of the TV notice, there is assurance that the notice will actually come to the attention of the class.

Lastly, the TV notice is informative, engaging, and easy to understand. And it allows class members to learn of their rights and options, and to act on them by visiting the settlement website.

In *Hinshaw v. Vizio*, the court preliminarily approved a class action settlement and notice plan which authorized Vizio to display a class action notice on Vizio TVs, among other notice. *See* No. 8:14-cv-00876-DOC (C.D. Cal.), Doc. 56 at § 7.3. Subsequently, the court granted final approval. *Hinshaw*, Doc. 69 at 3-4. Under that notice plan, the TV notice displayed a total of two times for 30 seconds unless the class member selected a command button to remove it. *Hinshaw*, Doc. 56 at § 7.3.

The TV Notice presented in this case is superior in that it will display more frequently for longer intervals. The TV Notice here also has the information demanded by Rule 23(c)(B)(2). And in contrast with the *Hinshaw* TV notice, the text of which is

represented in a single font-size, the text in the TV notice here is formatted to enhance class member engagement. We draw these comparisons not to diminish the TV Notice in *Hinshaw*, which satisfied Rule 23, but to explain the reasons why the design of the TV Notice in this case will be particularly effective.

Notice is also accomplished through a combination of e-mail, and digital and print media. Vizio has a large number of e-mail addresses. This reflects the manner in which customers engage Vizio. It also reflects "contemporary communication realities" of this particular demographic. Approximately 9,000,000 potential Settlement Class Members will receive the notice via e-mail. A.B. Data implements certain best practices to increase deliverability and bypass SPAM and junk filters and can verify the number of e-mails successfully delivered.[24]

Other forms of notice, such as the digital and print media campaign, will provide more than adequate coverage in the event that the outreach of the e-mail and TV notice reaches fewer settlement class members than estimated. Digital banners ads through the Google Display Network, Facebook (which includes a settlement-specific Facebook page) and Google AdWords/Search platforms will yield a minimum of 62 million impressions. Utilizing the known contact information and demographics of the settlement class, the digital banner ads will be specifically targeted to settlement class members and likely settlement class members.

Notice of the proposed settlement will be sent to relevant state and federal authorities per the terms of 28 U.S.C. § 1715(b) at least 90 days prior to the date for the final fairness hearing. 28 U.S.C. § 1715(d). A declaration attesting to this fact will be submitted to the Court.

Under Rule 23, the notice must include, in a manner that is understandable to potential class members: "(i) the nature of the action; (ii) the definition of the class certified; (iii) the class claims, issues, or defenses; (iv) that a class member may enter an

[24] Plaintiffs have provided the Court with mock ups of the TV and e-mail notice, so that the Court can review the notice in a similar manner in which it will be presented to the class.

appearance through an attorney if the member so desires; (v) that the court will exclude from the class any member who requests exclusion; (vi) the time and manner for requesting exclusion; and (vii) the binding effect of a class judgment on members under Rule 23(c)(3)." Fed. R. Civ. P. 23(c)(2)(B). This information is included in each of the notices in language that is easy to understand.

Because the class notices and notice plan set forth in the settlement agreement satisfy the requirements of due process and Federal Rule of Civil Procedure 23, and provide the best notice practicable under the circumstances, the Court should direct the parties and the Settlement Administrator to proceed with providing notice to settlement class members pursuant to the terms of the settlement agreement and its order granting preliminary approval.

V. CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court enter the proposed Preliminary Approval Order, thereby:

(1) preliminarily approving the proposed Settlement;

(2) provisionally certifying the proposed Settlement Class;

(3) appointing Plaintiffs as Class Representatives;

(4) appointing Class Counsel as Settlement Class Counsel;

(5) approving Plaintiffs' proposed notice program and directing that the notice be carried out under that program;

(6) appointing A.B. Data, Ltd. as Settlement Administrator and directing it to carry out the duties and responsibilities stated in the Settlement;

(7) approving Electronic Privacy Information Center, Privacy Rights Clearinghouse, and World Privacy Forum as next-best recipients of residual funds that cannot feasibly be distributed to class members; and

(8) setting a Final Approval Hearing and certain other dates in connection with the settlement approval process.

Respectfully submitted,

GIBBS LAW GROUP LLP

/s/ Andre M. Mura

Eric H. Gibbs
ehg@classlawgroup.com
Andre M. Mura
amm@classlawgroup.com
Linda Lam
lpl@classlawgroup.com
505 14th Street, Suite 1110
Oakland, CA 94612
Tel: (510) 350-9700
Fax: (510) 350-9701

COTCHETT, PITRE & MCCARTHY, LLP

/s/ Adam J. Zapala

Joseph W. Cotchett
jcotchett@cpmlegal.com
Adam J. Zapala
azapala@cpmlegal.com
840 Malcolm Road, Suite 200
Burlingame, CA 94010
Tel: (650) 697-6000
Fax: (650) 697-0577

Interim Co-Lead Counsel for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

KYLE ZAK, individually and on behalf of all others similarly situated, *Plaintiff*, *v.* BOSE CORP., a Delaware corporation, *Defendant.*	Case No. 17-cv-2928

CLASS ACTION COMPLAINT AND DEMAND FOR JURY TRIAL

Plaintiff Kyle Zak ("Zak" or "Plaintiff") brings this Class Action Complaint and Demand for Jury Trial against Defendant Bose Corp. ("Bose" or "Defendant") for secretly collecting, transmitting, and disclosing its customers' private music and audio selections to third parties, including a data mining company. Plaintiff, for his Complaint, alleges as follows upon personal knowledge as to himself and his own acts and experiences, and as to all other matters, upon information and belief, including investigation conducted by his attorneys.

NATURE OF THE ACTION

1. Defendant Bose manufactures and sells high-end wireless headphones and speakers. To fully operate its wireless products, customers must download Defendant's "Bose Connect" mobile application from the Apple App or Google Play stores and install it on their smartphones. With Bose Connect, customers can "pair" their smartphones with their Bose wireless products, which allows them to access and control their settings and features.

2. Unbeknownst to its customers, however, Defendant designed Bose Connect to (i) collect and record the titles of the music and audio files its customers choose to play through their Bose wireless products and (ii) transmit such data along with other personal identifiers to third-parties—including a data miner—without its customers' knowledge or consent.

3. Though the data collected from its customers' smartphones is undoubtedly valuable to the company, Defendant's conduct demonstrates a wholesale disregard for consumer privacy rights and violates numerous state and federal laws.

4. Indeed, one's personal audio selections – including music, radio broadcast, Podcast, and lecture choices – provide an incredible amount of insight into his or her personality, behavior, political views, and personal identity. In fact, numerous scientific studies show that musical preferences reflect explicit characteristics such as age, personality, and values, and can likely even be used to identify people with autism spectrum conditions.[1] And that's just a small sampling of what can be learned from one's music preferences. When it comes other types of audio tracks, the personality, values, likes, dislikes, and preferences of the listener are more self-evident. For example, a person that listens to Muslim prayer services through his headphones or speakers is very likely a Muslim, a person that listens to the Ashamed, Confused, And In the Closet Podcast is very likely a homosexual in need of a support system, and a person that listens to The Body's HIV/AIDS Podcast is very likely an individual that has been diagnosed and is living with HIV or AIDS. None of Defendant's customers could have ever anticipated that these types of music and audio selections would be recorded and sent to, of all people, a third party data miner for analysis.

5. As such, Plaintiff brings this suit individually and on behalf of all others similarly situated and seeks (i) an injunction prohibiting Bose from collecting, transmitting, and disclosing consumers' music and audio selections, (ii) actual and statutory damages arising from the invasion of their privacy, and (iii) actual damages arising from their purchase of the Bose

[1] Greenberg DM, Baron-Cohen S, Stillwell DJ, Kosinski M, Rentfrow PJ (2015) Musical Preferences are Linked to Cognitive Styles. PLoS ONE 10(7): e0131151. https://doi.org/10.1371/journal.pone.0131151.

Wireless Products, including the return of the purchase price of the product and disgorgement of profits.

PARTIES

6. Plaintiff Kyle Zak is a natural person and a citizen of the State of Illinois.

7. Defendant Bose Corporation is a corporation organized and existing under the laws of the State of Delaware with its principal place of business located at The Mountain, Framingham, Massachusetts 01701.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over Plaintiff's claim under the Wiretap Act, 18 U.S.C. § 2510, a federal statute, and supplemental jurisdiction over Plaintiff's state law claims because they are so related to Plaintiff's federal claim that they form part of the same case or controversy under Article III of the United States Constitution. The Court also has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2), because (i) at least one member of the Class is a citizen of a different state than the Defendant, (ii) the amount in controversy exceeds $5,000,000, exclusive of interests and costs, and (iii) none of the exceptions under that subsection apply to this action.

9. This Court has personal jurisdiction over Defendant because it conducts business in the State of Illinois and because the events giving rise to this lawsuit occurred, in substantial part, in the State of Illinois.

10. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred, in substantial part, in this District and Plaintiff resides in this District.

COMMON FACTUAL ALLEGATIONS

A Brief Overview of Defendant Bose and The Bose Connect App

11. In 2016, Bose introduced a new feature for some of its products that enabled customers to remotely control certain Bose headphones and speakers from their smartphones, including the QuietComfort 35, SoundSport Wireless, Sound Sport Pulse Wireless, QuietControl 30, SoundLink Around-Ear Wireless Headphones II, and SoundLink Color II ("Bose Wireless Products").

12. Bose customers could download Defendant's proprietary Bose Connect app from the Apple App Store or the Google Play Store and install it on their smartphones to take advantage of this new remote control feature.

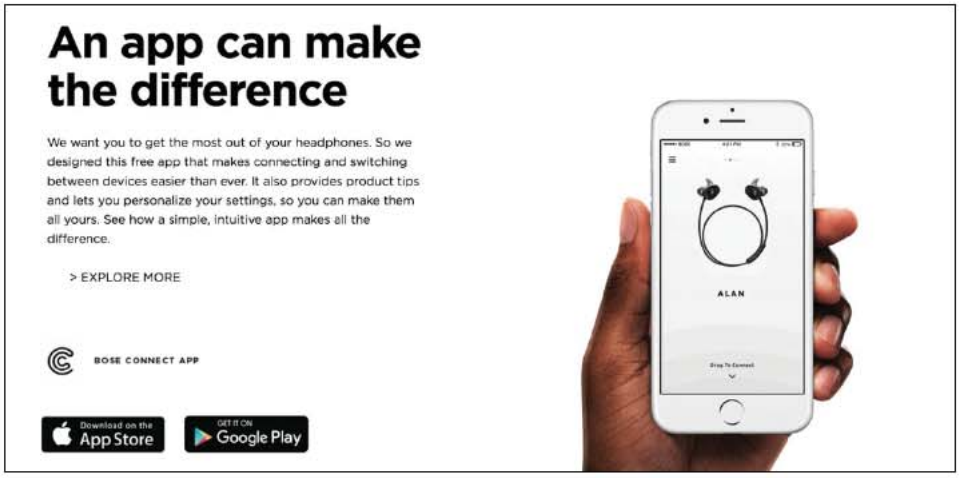
13. Once downloaded, the Bose Connect app allows customers to "pair" (i.e., connect) their Bose Wireless Products to their smartphones using a Bluetooth connection, and access essential product functionality. Specifically, through the Bose Connect app, customers can (i) download and install firmware updates to the Bose Wireless Products, (ii) manage the connections between the Bose Wireless Products and mobile devices, (iii) adjust the Bose Wireless Products' noise cancellation settings, (iv) customize the Bose Wireless Products' "Auto-Off" settings (for purposes of conserving the product's battery life), and (v) share music between two Bose Wireless Products.[2]

14. Users can utilize the Bose Connect app to pause, resume, rewind, and skip songs already playing on their smartphones. The Bose Connect app is not a music player like the iTunes or Podcast players found on Apple devices—it is simply a companion app that allows customers to remotely control their Bose Wireless Products.

[2] *Bose Connect on the App Store*, https://itunes.apple.com/us/app/bose-connect/id1046510029 (last visited April 18, 2017).

15. Defendant advertised the Bose Connect app functionality on the outside packaging of all Bose Wireless Products. For instance, the packaging of its SoundSport wireless headphones states in multiple languages: "[t]he Bose Connect app unlocks current and future headphone features. Download now."

16. Likewise, Defendant touts the functionality Bose Connect on its website, and invites consumers to download the app to "get the most out of your headphones." Defendant explains that Bose Connect "makes connecting and switching between devices easier than ever. It also provides product tips and lets you personalize your settings." *See* Figure 1.



(**Figure 1.**)[3]

17. Defendant also encourages its customers to register their Bose Wireless Products with Bose. Registered product owners will receive "confirmation of ownership" and "important updates for products."[4] During product registration, consumers provide their Bose Wireless Product's serial number, full name, email address, and phone number.

---

[3] *QC35 Wireless Noise Cancelling Headphones | Bose*, https://www.bose.com/en_us/products/headphones/over_ear_headphones/quietcomfort-35-wireless.html (last visited April 18, 2017).

[4] *Product registration*, https://www.bose.com/en_us/support/product_registration.html (last visited April 18, 2017).

Defendant Designed the Bose Connect App to Secretly Collect Consumers' Usage Data

18. As described above, customers must download and install Bose Connect to take advantage of the Bose Wireless Products' features and functions. Yet, Bose fails to notify or warn customers that Bose Connect monitors and collects—in real time—the music and audio tracks played through their Bose Wireless Products. Nor does Bose disclose that it transmits the collected listening data to third parties.

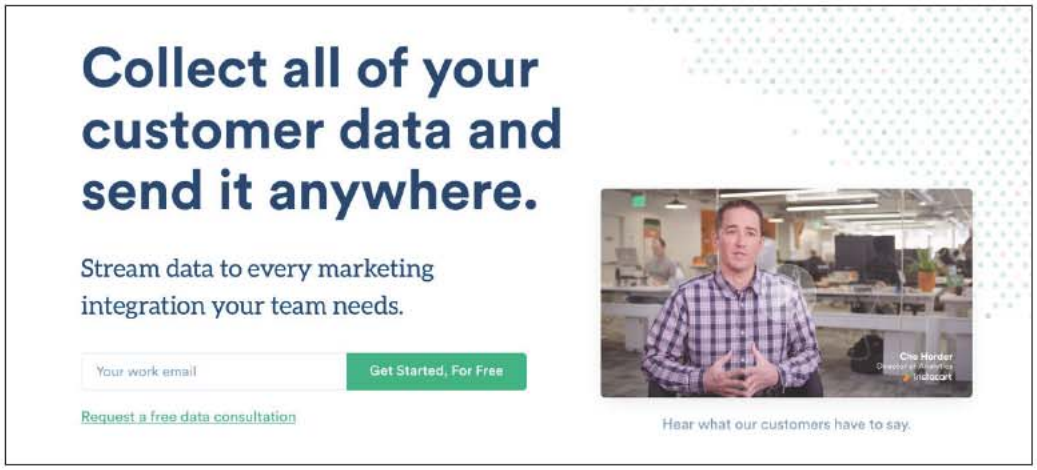
19. Indeed, Defendant programmed its Bose Connect app to continuously record the contents of the electronic communications that users send to their Bose Wireless Products from their smartphones, including the names of the music and audio tracks they select to play along with the corresponding artist and album information, together with the Bose Wireless Product's serial numbers (collectively, "Media Information").

20. As mentioned above, Bose solicits registration information (name and email address) and collects that information with the product's serial number. And by collecting the Bose Wireless Products' serial numbers along with Media Information, Bose is able to link the Media Information to any individual that has registered or will register their products, thus enabling Bose to create detailed profiles about its users and their music listening histories and habits.

21. To collect customers' Media Information, Defendant designed and programmed Bose Connect to continuously and contemporaneously intercept the content of electronic communications that customers send to their Bose Wireless Products from their smartphones, such as operational instructions regarding the skipping and rewinding audio tracks and their corresponding titles. In other words, when a user interacted with Bose Connect to change their audio track, Defendant intercepted the content of those electronic communications.

22. Defendant also intentionally designed and programmed its Bose Connect app to automatically disclose and transmit its customers' Media Information to third party companies, including a data miner called Segment.io, Inc. ("Segment.io").

23. According to its homepage, Segment.io is a sophisticated data mining and analysis company that can be used to "Collect all of your customer data and send it anywhere." *See* Figure 2.



(**Figure 2.**)[5]

24. The music and audio tracks that people listen to (i.e., Media Information) reveal sensitive information about themselves that suggests their politics, religious views, thoughts, sentiments, and emotions. In other words, knowing what music, radio broadcasts, lectures, and Podcasts a person chooses to listen to is enough to make accurate judgments and predictions about their personalities and behaviors.[6]

---

[5] *Analytics API and Customer Data Platform | Segment*, https://segment.com/ (last visited April 18, 2017).

[6] *Music and Personality*, https://www.verywell.com/music-and-personality-2795424 (last visited April 18, 2017) ("researchers found that people could make accurate judgments about an individual's levels of extraversion, creativity and open-mindedness after listening to ten of their favorite songs.")

25. Defendant never obtained consent from any of its customers before intercepting, monitoring, collecting, and transmitting their Media Information. To the contrary, Defendant concealed its actual data collection policies from its customers knowing that (i) a speaker or headphone product that monitors, collects, and transmits users' private music and audio tracks to any third party—let alone a data miner—is worth significantly less than a speaker or headphone product that does not, and (ii) few, if any, of its customers would have purchased a Bose Wireless Product in the first place had they known that it would monitor, collect, and transmit their Media Information.

FACTS SPECIFIC TO PLAINTIFF ZAK

26. On or around March 2017, Plaintiff Zak purchased Bose QuietComfort 35 wireless headphones for $350.

27. Immediately after he purchased the headphones, Plaintiff registered his product with Bose and downloaded the Bose Connect app onto his smartphone in order to access the headphone's full array of features. During the registration process, Plaintiff provided Bose with his product's unique serial number, as well as his full name and email address.

28. Plaintiff uses his smartphone several times each day to select music tracks to play through his Bose wireless headphones, and often opens the Bose Connect app while such music is playing to configure the settings, access additional features, and to skip and pause audio tracks.

29. Unbeknownst to Plaintiff, each and every time he opened Bose Connect, Defendant intercepted and collected all available Media Information from his smartphone—including the names of any music and audio tracks he played through his wireless headphones and his personally identifiable serial number—and transmitted such information to third parties, including to data miner Segment.io.

30. Plaintiff Zak never provided his consent to Bose to monitor, collect, and transmit his Media Information. Nor did Plaintiff ever provide his consent to Bose to disclose his Media Information to any third party, let alone data miner Segment.io.

31. Likewise, Defendant never informed Plaintiff Zak that it would monitor, collect, transmit, and disclose his Media Information.

32. Plaintiff Zak would never have purchased his Bose Wireless Product had he known that Defendant would use Bose Connect (which was necessary to access the product's full array of functions and features) to collect, transmit, and disclose his Media Information.

CLASS ALLEGATIONS

33. **Class Definitions:** Plaintiff brings this action pursuant to the Federal Rules of Civil Procedure 23(b)(2) and 23(b)(3) on behalf of himself and a class and subclass of similarly situated individuals as follows:

> **Class:** All individuals in the United States who purchased a Bose Wireless Product and installed the Bose Connect mobile app.
>
> **Illinois Subclass:** All members of the Class who are domiciled in the State of Illinois.

The following people are excluded from the Classes: (1) any Judge or Magistrate presiding over this action and the members of their family; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and their current or former employees, officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Classes; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

34. **Numerosity**: The exact number of members of the Classes is unknown, but

individual joinder in this case is impracticable. The Classes likely consist of tens of thousands of individuals. Members of the Classes can be easily identified through Defendant's records and/or Defendant's retail partners' records.

35. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the other members of the Classes, and those questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include but are not limited to the following:

(a) Whether Defendant's conduct constitutes a violation of the Wiretap Act;

(b) Whether Defendant's conduct constitutes a violation of the Illinois Eavesdropping Statute;

(c) Whether Defendant's conduct constitutes an intrusion upon seclusion;

(d) Whether Defendant was unjustly enriched through its conduct; and

(e) Whether Defendant's conduct constitutes a violation of the Illinois Consumer Fraud and Deceptive Business Practice Act.

36. **Typicality**: Plaintiff's claims are typical of the claims of the other members of the Classes in that Plaintiff and the members of the Classes sustained damages arising out of Defendant's uniform wrongful conduct.

37. **Adequate Representation**: Plaintiff has and will continue to fairly and adequately represent and protect the interests of the Classes, and they have retained counsel competent and experienced in complex litigation and class actions. Plaintiff has no interests antagonistic to those of the Classes, and Defendant has no defenses unique to Plaintiff. Plaintiff and his counsel are committed to vigorously prosecuting this action on behalf of the members of the Classes, and they have the resources to do so. Neither Plaintiff nor their counsel have any interest adverse to those of the other members of the Classes.

38. **Superiority**: This class action is also appropriate for certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy and joinder of all members of the Classes is impracticable. The damages suffered by the individual members of the Classes will likely be small relative to the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's wrongful conduct. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

FIRST CAUSE OF ACTION
Violation of the Federal Wiretap Act
18 U.S.C. § 2510 *et seq.*
(On behalf of Plaintiff and the Class)

39. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

40. The Wiretap Act generally prohibits the intentional "interception" of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1)(a). The Act also prohibits the intentional disclosure of such communications. 18 U.S.C. § 2511(1)(c).

41. By designing the Bose Connect app to contemporaneously and secretly collect Media Information—including details about the music played by Plaintiff and the Class members—Defendant Bose intentionally intercepted and/or endeavored to intercept the contents of "electronic communications" in violation of 18 U.S.C. § 2511(1)(a).

42. Further, by automatically and contemporaneously transmitting and disclosing the content of an electronic communication it collected from Plaintiff and the Class members to a third-party company while knowing or having reason to know that the data was obtained through the interception of an electronic communication, Defendant violated 18 U.S.C. § 2511(1)(c).

43. No party to the electronic communications alleged herein consented to Defendant's collection, interception, use, or disclosure of the contents of the electronic communications. Nor could they—Defendant never sought to obtain Plaintiff's and the Class's consent, nor did Defendant obtain the consent of the other party, such as Spotify or other media providers. Moreover, Defendant was not a party to any of the electronic communications sent and/or received by Plaintiff and members of the Class.

44. Plaintiff and the Class suffered harm as a result of Defendant's violations of the Wiretap Act, and therefore seek (a) preliminary, equitable, and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendant as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Violation of the Illinois Eavesdropping Statute
720 ILCS 5/14-1 *et seq*.
(On behalf of Plaintiff and the Illinois Subclass)

45. Plaintiff incorporates the foregoing allegation as if fully set forth herein.

46. A person violates the Illinois Eavesdropping Statute when he or she knowingly and intentionally "[i]ntercepts, records, or transcribes, in a surreptitious manner any private electronic communication to which he or she is not a party unless he or she does so with the consent of all parties to the private electronic communication. . . ." 720 ILCS 5/14-2(a).

47. The statute broadly defines "private electronic communication" to mean "any

transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or part by a wire, radio, pager, computer, electromagnetic, photo electronic or photo optical system, when the sending or receiving party intends the electronic communication to be private under circumstances reasonably justifying that expectation." 720 ILCS 5/14-1(e).

48. By designing and programming the Bose Connect app to contemporaneously monitor, intercept, collect, record, transmit, and disclose the contents of private electronic communications that Plaintiff and the Illinois Subclass sent Bose Wireless Products and their smartphone operating systems—including the music and audio tracks they selected to play—Defendant intentionally and knowingly monitored, intercepted, collected, recorded, transmitted, and disclosed "private electronic communications," in violation of 720 ILCS 5/14-2.

49. Plaintiff and the Illinois Subclass members intended that their Media Information would be private. Indeed, their Media Information reveals highly sensitive details about their private use of their personal headphones and speakers that Plaintiff and the Illinois Subclass expected to remain private and confidential. Beyond that, Defendant never notified Plaintiff and the Illinois Subclass that it was monitoring, intercepting, or disclosing their Media Information. Thus, there was no reason for them to believe that anybody could even potentially access, intercept, or disclose their private electronic communications in the first place.

50. Neither Plaintiff nor the members of the Illinois Subclass ever consented to Defendant's interception, collection, recording, use, or disclosure of their private electronic communications.

51. As a result of Defendant's unlawful conduct, Plaintiff and the members of the Illinois Subclass have been injured and seek: (1) an injunction prohibiting further eavesdropping by Defendant, (2) actual damages, including the amount paid for the Bose Wireless Products,

and (3) punitive damages in an amount to be determined by the court or by a jury pursuant to 720 ILCS 5/14-6(c).

THIRD CAUSE OF ACTION
Intrusion Upon Seclusion
(On behalf of Plaintiff and the Illinois Subclass)

52. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

53. As explained herein, Defendant has intruded upon the seclusion of Plaintiff and each member of the Illinois Subclass by secretly monitoring, collecting, transmitting, and disclosing their Media Information, which revealed specific details regarding their music and audio selections, preferences, and habits.

54. By designing and programming Bose Connect to secretly monitor, intercept, transmit, and disclose its customers' Media Information, Defendant intentionally and knowingly intruded upon the seclusion of Plaintiff's and Illinois Subclass members' private affairs.

55. Further, Defendant's monitoring, collection, transmission, and disclosure of Plaintiff's and Illinois Subclass members' Media Information—without their knowledge or consent—is highly offensive to a reasonable person as it is capable of revealing highly private details about their lives, including *inter alia* their personalities, behavior, and political affiliations and views, which they believed were confidential, and had no reason whatsoever to suspect that anybody would be spying on their music and audio selections.

56. Defendant's intrusion upon Plaintiff's and the Illinois Subclass members' privacy caused them to mental anguish and suffering in the form of anxiety and concern regarding the safety and whereabouts of their Media Information.

57. Plaintiff, on his own behalf and on behalf of the Illinois Subclass, seeks (1) an injunction that prohibits Defendant from monitoring, transmitting, or disclosing their Media

Information without informed consent, (2) actual damages, including the amount paid for the Bose Wireless Products, and (3) punitive damages, as well as for costs and reasonable attorneys' fees incurred.

FOURTH CAUSE OF ACTION
Violation of the Illinois Consumer Fraud and Deceptive Business Practice Act
815 ILCS 505/1 *et seq*.
(On behalf of Plaintiff and the Illinois Subclass)

58. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

59. The Illinois Consumer Fraud and Deceptive Business Practices Act, 815 ILCS 505/1 et seq. ("ICFA") protects both consumers and competitors by promoting fair competition in commercial markets for goods and services.

60. The ICFA prohibits any unlawful, unfair, or fraudulent business acts or practices including the employment of any deception, fraud, false pretense, false promise, false advertising, misrepresentation, or the concealment, suppression, or omission of any material fact.

61. The ICFA applies to Defendant's conduct as described herein because it protects consumers in transactions that are intended to result, or which have resulted, in the sale of goods or services.

62. Defendant is a "person" as defined by 505/1(c) because it is a corporation.

63. Plaintiff and the Illinois Subclass members are "consumers" as defined by 505/1(e) because they purchased merchandise—the Bose Wireless Products—for their own use.

64. Defendant's Bose Wireless Products are "merchandise" as defined by 505/1(b) and their sale is considered "trade" or "commerce" under the ICFA.

65. Defendant violated the ICFA by concealing material facts about their Bose Wireless Products and the Bose Connect app. Specifically, Defendant omitted and concealed that Bose Connect secretly monitors, collects, transmits, and discloses its users' highly private and

sensitive Media Information to third parties, including data miners.

66. Defendant's data interception, collection, and disclosure practices are material to the transactions here. Defendant featured its Bose Connect app in its marketing and advertising, offered certain features and functions to customers that were only available through Bose Connect, and charged a higher price for its Bose Wireless Products relative to comparable, non-Bluetooth products. Had Plaintiff and the Illinois Subclass known the true characteristics and behavior of the device (that it collects, transmits, and discloses private usage data to third parties, including data miners), they would not have purchased the Bose Wireless Products or would have paid substantially less for them.

67. Defendant intentionally concealed the Bose Wireless Products' collection, transmission, and disclosure practices because it knew that consumers would not otherwise purchase their products. Indeed, Defendant's concealment of such facts was intended to mislead consumers.

68. Defendant's concealment, suppression, and omission of material facts was likely to mislead reasonable consumers under the circumstances, and thus constitutes an unfair and deceptive trade practice in violation of the ICFA.

69. Thus, by failing to disclose and inform Plaintiff and the Illinois Subclass about its data collection practices, Defendant violated section 505/2 of the ICFA.

70. As a direct and proximate result of these unfair and deceptive practices, Plaintiff and each Illinois Subclass member has suffered actual harm in the form of money paid for a product that they would not have purchased had they known it would monitor, collect, transmit, and disclose Media Information to the third parties, including data miners.

71. As such, Plaintiff and the Illinois Subclass, seeks an order (1) requiring Defendant

to cease the unfair practices described herein, (2) awarding actual damages, including the amount paid for the Bose Wireless Products, and (3) awarding reasonable attorneys' fees and costs.

FIFTH CAUSE OF ACTION
Unjust Enrichment
(On behalf of Plaintiff and the Class)

72. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

73. Plaintiff and the Class members conferred a benefit on to Defendant Bose when they purchased their Bose Wireless Products.

74. Defendant Bose appreciates and/or has knowledge of such benefit.

75. Given that Defendant monitored, collected, transmitted, and disclosed Plaintiff's and the Class's Media Information without their knowledge or consent—and because Plaintiff and the Class would never have purchased the product had they known that such information would be accessible and disclosed to third parties, including a data miner—Defendant has unjustly received and retained a benefit as a result of its conduct.

76. Principles of equity and good conscience require Bose to return the purchase price of the Bose Wireless Products to Plaintiff and the Class.

77. Plaintiff and the Class members seek disgorgement and restitution of any money received by Defendant as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Kyle Zak, on behalf of himself and the Class, and the Illinois Subclass requests that the Court enter an Order:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Kyle Zak as a representative of the Classes, and appointing his counsel as class counsel;

B. Declaring that Defendant's actions violate the Wiretap Act, the Illinois Eavesdropping Statute, and the Illinois Consumer Fraud and Deceptive Business Practices Act, and that they constitute an Intrusion Upon Seclusion and Unjust Enrichment;

C. Awarding injunctive relief that (i) prohibits Defendant from collecting, monitoring, transmitting, or disclosing Plaintiff's and the Classes' Media Information without consent, and (ii) requires Defendant and any third parties with such information in their possession, including Segment.io, to destroy it immediately;

D. Awarding damages, including actual, statutory, and punitive damages, to Plaintiff and the Classes in an amount to be determined at trial;

E. Awarding Plaintiff and the Classes their reasonable attorneys' fees and expenses;

F. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable;

G. Awarding such and other injunctive and declaratory relief as is necessary to protect the interests of Plaintiff and the Classes; and

H. Awarding such other and further relief as the Court deems reasonable and just.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Dated: April 18, 2017

Respectfully submitted,

KYLE ZAK, individually and on behalf of all other similarly situated,

By: /s/ Benjamin S. Thomassen
One of Plaintiff's Attorneys

Jay Edelson
jedelson@edelson.com
Benjamin S. Thomassen
bthomassen@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel: 312.589.6370
Fax: 312.589.6378

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET AND TECHNOLOGY

In the Matter of

Assurance No. 17-056

Investigation by ERIC T. SCHNEIDERMAN, Attorney General of the State of New York, of

SAFETECH PRODUCTS, LLC, and RYAN HYDE, as an individual,

Respondents.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York ("NYAG") commenced an investigation pursuant to Executive Law § 63(12) and General Business Law ("GBL") §§ 349 and 350 into the security of Safetech Products LLC, and its owner Ryan Hyde ("Respondents"), Bluetooth-enabled locks. This Assurance of Discontinuance ("Assurance") contains the findings of the NYAG's investigation and the relief agreed to by NYAG and Respondents.

FINDINGS OF NYAG

1. Safetech Products, LLC ("Safetech" is a limited liability corporation with a principal place of business at 1601 North State Street, Lehi, Utah. It is owned by Ryan Hyde.

2. Safetech sells Bluetooth-enabled locks to customers through its website https://www.thequicklock.com/ with the promise "Privacy When You Want It, Security When You Need It." With Bluetooth-enabled locks, the user may control the locks with an application ("app") installed on a smartphone.

3. Bluetooth is a wireless technology standard for exchanging data over short distances of up to 300 feet. It uses short-wavelength UHF radio waves in the ISM band from 2.4

to 2.485 GHz. To operate the Bluetooth-enabled lock, the smartphone and the lock must have their Bluetooth antennas turned on at the same frequency band and broadcast their identifiers to each other. A default password is used to secure the connection and exchange data.

4. In August 2016, independent security researchers reported that Respondents' Bluetooth-enabled locks transmitted passwords between the locks and the user's smartphone in plain text and without encryption. The researchers reported that a wrong-doer could intercept the passwords and proceed to unlock the locks. The researchers also reported that the locks contained weak default passwords that were not secure and could be guessed or discovered through brute force attacks (i.e., automated software used to generate a large number of consecutive guesses).

5. In October 2016, the NYAG contacted Respondents about the findings of the researchers and the security of the locks. Just prior to being contacted by the NYAG, Respondents voluntarily placed the following warning on the https://www.thequicklock.com/ website:

> SECURITY WARNING...Bluetooth keys for the hardware are passed "unencrypted" on all current products.
>
> We also strongly recommend the default password be changed at initial setup. Please read "Security Risks Explained."

Upon clicking the "Security Risks Explained" hyperlink, the user is taken to a webpage that explains the risks identified above.

6. Respondents' locks limited the Bluetooth range to approximately 50 feet. Thus, a wrongdoer would need to be in close proximity to the lock to intercept the Bluetooth passwords. Additionally, the locks shutdown for 2 minutes with two failed password attempts. Thus, a brute force attack would be limited by the locks 2-minute lock-out feature.

7. By violating express and implied representations of reasonable data security, Respondents violated New York Executive Law § 63(12) and New York General Business Law §§ 349 and 350.

PROSPECTIVE RELIEF

WHEREAS, Respondents admit NYAG Findings (1)-(6) above;

WHEREAS, NYAG is willing to accept the terms of this Assurance pursuant to Executive Law § 63(15) and to discontinue its investigation into Respondents' representations concerning the security of its Bluetooth-enabled locks; and

WHEREAS, the parties each believe that the obligations imposed by this Assurance are prudent and appropriate;

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the parties, that:

8. This Assurance shall apply to Respondent Safetech Products LLC, and any officers, directors, servants, agents, employees, assignees, and any individual, subsidiary, division, or other entity through which the company may now or hereafter act, as well as any successors-in-interest, and Ryan Hyde, as an individual.

9. Respondents shall comply with Executive Law § 63(12), and GBL §§ 349 and 350, and shall not misrepresent, expressly or by implication, the security of its locks, or the security, confidentiality, or integrity of any data these devices transmit via Bluetooth or other radio frequencies.

10. Respondents shall encrypt all passwords, electronic keys or other credentials ("Security Information") in their locks and other Bluetooth-enabled devices that Respondents market or sell to individual consumers and the general public. Respondents' Bluetooth-enabled

devices shall prompt users to change the default password upon the customer's initial setup of wireless communication.

11. Within 30 days of the execution of this Assurance, Respondents shall establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing devices that use Security Information, and (2) protect the privacy, security, confidentiality, and integrity of Security Information. Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards appropriate to company's size and complexity, the nature and scope of the company's activities, and the sensitivity of the device's function or the information it collects, transmits or processes, including:

a. The designation of an employee or employees to coordinate and be accountable for the security program;

b. The identification of material internal and external risks to (1) the security of the devices that could result in unauthorized access to or unauthorized modification of the device and (2) the privacy, security, confidentiality, and integrity of Security Information;

c. The risk assessments required by subpart b must include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing; (4) review, assessment, and response to third party security vulnerability

reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

d. The design and implementation of reasonable safeguards to control the risks identified through risk assessment;

e. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures including reasonable and appropriate security testing techniques such as vulnerability and penetration testing, security architecture reviews and code reviews;

f. The development and use of reasonable steps to select and retain service providers (if any are hired) capable of maintaining security practices consistent with this Assurance, and requiring service providers by contract to implement and maintain appropriate safeguards consistent with this Assurance; and

g. The evaluation and adjustment of Respondents' security program in light of the results of the testing and monitoring required by subpart e, any material changes to Respondents' operations or business arrangements, or any other circumstances that Respondents' knows or has reason to know may have a material impact on the effectiveness of the security program.

12. Respondents shall, within 10 business days of receiving a written request from NYAG, make available for NYAG review a copy of Respondents' written policies and procedures adopted pursuant to this Assurance or otherwise.

Miscellaneous

13. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondents and its counsel and NYAG's own factual

investigation as set forth in Findings (1)-(6) above. To the extent that any of Respondents' representations are later found to be inaccurate or misleading, this Assurance is voidable by the NYAG in its sole discretion.

14. If the Assurance is voided or breached, Respondents agree that any statute of limitations or other time-related defenses applicable to the subject of the Assurance and any claims arising from or relating thereto are tolled from and after the date of this Assurance. In the event the Assurance is voided or breached, Respondents expressly agree and acknowledge that this Assurance shall in no way bar or otherwise preclude NYAG from commencing, conducting or prosecuting any investigation, action or proceeding, however denominated, related to the Assurance, against the Respondents, or from using in any way any statements, documents or other materials produced or provided by Respondents prior to or after the date of this Assurance.

15. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondents in agreeing to this Assurance.

16. Respondents represent and warrant, through the signatures below, that the terms and conditions of this Assurance are duly approved, and execution of this Assurance is duly authorized. Respondents shall not take any action or make any statement denying, directly or indirectly, the propriety of this Assurance or expressing the view that this Assurance is without factual basis. Nothing in this paragraph affects Respondents' (i) testimonial obligations or (ii) right to take legal or factual positions in defense of litigation or other legal proceedings to which NYAG is not a party. This Assurance may not be used and is not intended for use by any third party in any other proceeding.

17. This Assurance may not be amended except by an instrument in writing signed on

behalf of all the parties to this Assurance.

18. This Assurance shall be binding on and inure to the benefit of the parties to this Assurance and their respective successors and assigns, provided that no party, other than NYAG, may assign, delegate, or otherwise transfer any of his rights or obligations under this Assurance without the prior written consent of NYAG.

19. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held to be invalid, illegal, or unenforceable in any respect, in the sole discretion of the NYAG such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

20. To the extent not already provided under this Assurance, Respondents shall, upon request by NYAG, provide documentation and information necessary for NYAG to verify compliance with this Assurance.

21. All notices, reports, requests, and other communications to any party pursuant to this Assurance shall be in writing and shall be directed as follows:

If to Respondents:

SafeTech Products, LLC
TheQuickLock LLC
1601 North State Street]
Lehi, Utah 84043

If to the NYAG, to:

Attorney General of the State of New York
120 Broadway
New York, New York 10271
Attention: Chief, Bureau of Internet and Technology

22. Acceptance of this Assurance by NYAG shall not be deemed approval by NYAG of any of the practices or procedures referenced herein, and Respondents shall make no

representation to the contrary.

23. Pursuant to Executive Law § 63(15), evidence of a violation of this Assurance shall constitute *prima facie* proof of violation of the applicable law in any action or proceeding thereafter commenced by NYAG.

24. If a court of competent jurisdiction determines that Respondents have breached this Assurance, Respondents shall pay to NYAG the cost, if any, of such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

25. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. The NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding.

26. This Assurance shall be governed by the laws of the State of New York without regard to any conflict of laws principles.

27. Nothing contained herein shall be construed as to deprive any person of any private right under the law.

28. This Assurance may be executed in counterparts, each of which shall be deemed to be an original, but all of which, taken together, shall constitute one and the same agreement.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

ERIC T. SCHNEIDERMAN
NEW YORK ATTORNEY GENERAL
BUREAU OF INTERNET AND TECHNOLOGY

By: Clark Russell
Deputy Bureau Chief

5/9/17
Date

SAFETECH PRODUCTS LLC AND RYAN HYDE

By:

May 3, 2017
Date

New York Attorney General's Office
120 Broadway
New York, NY 10271-0332
Phone: (212) 416-8433
Fax: (212) 416-8369

Expert Analysis

How The GDPR Changed Data Privacy In 2018

By **Jessica Lee**
December 14, 2018, 2:47 PM EST

Jessica Lee

The European Union General Data Protection Regulation became enforceable on May 25, 2018, bringing in a flurry of privacy notice updates, the shutdown of certain EU-facing websites and advertising activities, and a good amount of heartburn for companies within its territorial scope.

The threat of fines of up to 4 percent of a company's global revenue put a new spotlight on privacy and data protection, and caused a level of panic that was reminiscent of Y2K. Unlike Y2K, however, the road to GDPR compliance will extend well beyond its enforcement date.

What's Happened Since May?

In the past six months, compliance with the GDPR has moved from concept to reality, and both private citizens and data protection authorities, or DPAs, have taken action to enforce its requirements. Data subjects (individuals located in Europe) have started to enforce their rights, and DPAs have reported an increase in individual complaints.

Outside Europe, other countries have started to pass laws that mirror the GDPR's requirements, suggesting that at least some elements of the law may be our new global standard for privacy.

Enforcement Activity

As expected, tech companies have been among the first targets of GDPR enforcement activity. NOYB, a European consumer rights organization founded by Max Schrems, filed four lawsuits[1] against major tech companies the day GDPR went into effect, challenging the companies' consent mechanisms, and arguing that asking users to accept a company's privacy policies in order to access services violates the requirement that consent be "freely given."

In September, Dr. Johnny Ryan, chief policy and industry relations officer of Brave, a web browser that blocks ads and website trackers, filed a complaint[2] with several DPAs, asking them to investigate certain ad tech companies for "data breaches" caused by behavioral advertising. According to the press release, "every time a person visits a website and is shown a 'behavioural' ad on a website, intimate personal data that describes each visitor … is broadcast to tens or hundreds of companies … in order to solicit potential advertisers' bids for the attention of the specific individual visiting the website. A data breach occurs because this broadcast, known as a 'bid request' in the online industry, fails to protect these

intimate data against unauthorized access."

In late November, consumer groups across seven European countries filed complaints[3] against another major tech company, alleging that it does not have a lawful basis for processing location data, because its users are not given a real choice about how that data is used. DPAs in France and the United Kingdom have also issued warnings to several ad tech companies, challenging the consent mechanisms used for the collection of location data.

While fines have been issued, they have been limited. A €4,800 fine for illegal video surveillance activities and a €400,000 fine imposed on a hospital after employees illegally accessed patient data are among the few reported fines issued.[4] In Germany, a €20,000 fine was imposed on a social media platform after an investigation following a reported security breach revealed that the company stored user passwords in plain text. The violation of the obligation to guarantee the security of personal data under Article 32 (1)(a) of the GDPR, rather than the breach itself, was cited as the justification for the fine.[5]

Below are some lesson learned from enforcement activities of the past six months.

Warnings Before Fines — For Now

In many cases, DPAs have issued warning letters and notices, rather than fines. In July, for example, the U.K. Information Commissioner's Office (U.K. ICO) issued an enforcement notice[6] to AggregateIQ Data Services Ltd., or AIQ, a Canadian data analytics firm. AIQ was hired to target ads at voters during the Brexit referendum campaign.

Although AIQ used data that was collected prior to May 25, it retained and processed data after that date without having a lawful basis to do so, and without providing adequate transparency. The U.K. ICO alleged that by using this data to target individuals with political advertising on social media, AIQ "processed personal data in a way that those individuals were not aware or, for purposes which they would not have expected, and without a lawful basis for that processing." According to the BBC, AIQ plans to appeal the notice.

Although these warnings have been issued to specific companies, all companies subject to the GDPR should take note. Companies that fail to adjust their practices to meet the standards articulated in these warnings could ultimately be subject to fines.

Beware of Data Subject Complaints

Responding to data subject requests is one of the key elements of GDPR compliance, and one of the greatest sources of risk — a data subject's complaint may put a company on a DPA's radar for enforcement. The CNIL (France's DPA) reported that since May 2018, it has received over 3,000 complaints from individuals, and the Irish DPA also provided figures indicating that, as of July, it had logged 743 complaints.[7]

Prompted by a consumer complaint, the Irish Data Protection Commissioner recently initiated an investigation into t.co, Twitter's link-shortening system. Twitter allegedly declined to provide t.co data in response to the consumer's access request, arguing that to do so would require disproportionate effort.[8]

Provide Consumers a Choice Before Using Location Data for Advertising Purposes

Both regulators and consumer groups have focused on the use of location data in the warnings or complaints issued since May. In July, the CNIL announced[9] formal notice proceedings against Fidzup and Teemo — two mobile ad tech companies — for failing to obtain GDPR-compliant consent from individuals when processing their geolocation data for advertising purposes. (Teemo was also put on notice for retaining geolocation data for 13 months, which the CNIL said was too long to justify the purpose of targeted advertising.)

In each case, the individuals were asked to consent only to the collection of data by the mobile application, not the software development kit, or SDK. Additionally, the CNIL challenged the timing of the consent, finding that the SDK started to collect data upon installation of the app, before consent was obtained. In late October, a similar proceeding[10] was opened involving SingleSpot, another mobile ad tech company. All three proceedings have since been closed.[11]

Each company updated its practices to require its publisher partners to display a banner during the app installation process to give users the choice to opt in to any data collection. These banners inform users of the following: 1) the purpose of the data collection; 2) the identity of controllers receiving that data (accessible via hyperlink); 3) the data collected; and 4) the possibility of withdrawing consent at any time. Teemo also updated its data retention policies so that raw data is deleted after 30 days and aggregate data is deleted after 12 months.

Programmatic Advertising Survives, With New Restrictions

The IAB Europe's Transparency and Consent Framework, or TCF, a protocol for collecting consent and conveying it throughout the adtech ecosystem, is positioned to be the industry's most viable solution for consent management. That said, there continue to be some challenges, particularly in the context of programmatic advertising where the requirement to be "specific" about the various purposes for which data is being collected and the identity of the recipients makes it difficult to draft language that is clear and understandable enough to demonstrate that the consent is also "informed."

At the end of October, the CNIL issued a notice[12] to Vectaury, another mobile ad tech company, for its failure to obtain GDPR-compliant consent for its data processing activities. Vectaury collected data both through its SDK and through real-time bidding offers initially transmitted via auctions for advertising inventory. Vectaury retained the data it received through the bidding offers for use beyond responding to the bid. Although Vectaury implemented a consent management platform as part of the TCF, the CNIL found that the consent language failed to notify the users how their data would be used and who it would be shared with.

Small Companies Won't Escape Enforcement

It is worth noting that the initial actions by the U.K. ICO and CNIL have been directed towards small ad tech companies, confirming that it is the activity of a company, rather than its size, that will determine the likelihood of enforcement.

Legitimate Interests Remains Viable — For Now

In each of the cases involving the collection of geolocation data addressed by the CNIL, the company relied on consent as its lawful basis for processing data.

What has yet to be tested is whether, rather than trying to meet the stringent requirements for consent, ad tech companies may find a better path forward with another lawful basis, such as legitimate interests (at least for processing activities that don't involve sensitive or special categories of data).

Data Breach Reporting Has Increased and Individuals Have Exercised Their Rights

One of the key changes to European privacy law introduced by the GDPR is the 72 hour window for reporting personal data breaches. The CNIL reported[13] that since May 2018, it has received approximately seven data breach notifications a day involving 15 million individuals.

The Irish DPA also provided figures indicating that, as of July, it had logged 1,184 data breach notifications. According to Microsoft,[14] over five million people from 200 countries have used Microsoft's new privacy tools to manage their data, and over two million of those requests came from the U.S.

New Guidance on Territorial Scope

The European Data Protection Board, or EDPB, which replaced the Article 29 Working Party as the body in charge of ensuring that the GDPR is applied consistently across the European Union, issued draft guidance[15] on territorial scope. The guidance attempts to clarify that the processing of personal data of individuals in the EU by non-EU companies does not trigger the application of the GDPR, as long as the processing is not related (1) to a specific offer directed at individuals in the EU or (2) to a monitoring of their behavior in the EU.

The draft reinforces previous guidance that the mere accessibility of a website in the EU does not, by itself, provide sufficient evidence to demonstrate the controller's or processor's intention to offer goods or services to an individual located in the EU. With respect to monitoring, the EDPB does not consider that merely any online collection or analysis of personal data of individuals in the EU would automatically count as "monitoring."

Instead, it will consider the controller's purpose for processing the data and, in particular, any subsequent behavioral analysis or profiling techniques involving that data. Comments to the guidelines are due by Jan. 18, 2019.

What's Next?

In the next three to six months, we expect to see more enforcement action (including fines) as the DPAs work their way through pending complaints. In the long term, we expect that more countries will follow Brazil, India and California in passing "GDPR-like" regulations.

More than ever, understanding your data collection, use, storage and deletion practices is crucial so that you are prepared for these and future regulatory developments. Below are a few points to consider as your company prepares for 2019.

Data Mapping

Companies that didn't conduct a data-mapping exercise may consider doing so in 2019. Understanding what data you have, where it is stored, how it is used and to whom it is disclosed will put your organization ahead of the curve in complying with any new privacy regulations.

Ongoing Privacy Assessments

Data protection impact assessments drafted 6 months ago may already be out of date. Implementing an ongoing privacy assessment program will help privacy and business teams work together to manage the privacy risks presented by new projects.

Monitor Enforcement

Use the enforcement actions as a check against your company's practices. Companies may avoid enforcement by learning the lessons imposed on others.

Examine Security Practices

While companies have some flexibility to determine what level of technical and organizational security practices are appropriate for the nature of the data they process, security practices should at least align with industry best practices.

Jessica B. Lee is a partner at Loeb & Loeb LLP.

[1] https://noyb.eu/4complaints/.

[2] https://brave.com/adtech-data-breach-complaint.

[3] https://www.beuc.eu/publications/consumer-groups-across-europe-file-complaints-against-google-breach-gdpr/html.

[4] https://iapp.org/news/a/germanys-first-fine-under-the-gdpr-offers-enforcement-insights/.

[5] Id.

[6] https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf.

[7] https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application.

[8] http://fortune.com/2018/10/12/twitter-gdpr-investigation-tco-tracking/.

[9] https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-absence-de-consentement-geolocalisation-ciblage-publicitaire.

[10] https://www.cnil.fr/fr/applications-mobiles-mises-en-demeure-pour-absence-de-consentement-au-traitement-de-donnees-de.

[11] https://www.cnil.fr/fr/applications-mobiles-cloture-des-mises-en-demeure-lencontre-des-societes-fidzup-et-singlespot.

[12] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000037594451&fastReqId=974682228&fastPos=2.

[13] https://www.cnil.fr/fr/rgpd-quel-premier-bilan-4-mois-apres-son-entree-en-application.

[14] https://blogs.microsoft.com/on-the-issues/2018/09/17/millions-use-microsofts-gdpr-privacy-tools-to-control-their-data-including-2-million-americans/.

[15] https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf.

New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 259—NO. 42

MONDAY, MARCH 5, 2018

The GDPR: A Silver Lining For Data Governance

BY JESSICA B. LEE

SHUTTERSTOCK

The countdown to the enforcement date of the EU General Data Protection Regulation (GDPR) has begun and it's becoming increasingly clear that many U.S. organizations are poised to be caught in its crosshairs. Organizations that offer goods or services in the EU (whether or not a payment is involved) or that monitor the behavior of individuals in the EU, will be subject to the GDPR's requirements whether or not they have a presence in the EU. For U.S. organizations that are being exposed to the EU's regulatory regime for the first time, panic may be setting in (if it hasn't already). Requirements around honoring expanded data subject rights, maintaining records of processing, documenting the legal basis for such processing, and complying with the new security breach notification requirements, among others, may be particularly challenging for organizations that don't have well–developed data governance policies or centralized systems and databases.

The GDPR replaces the previous Data Protection Directive 95/46/EC (the Directive) as the governing privacy regulation in the EU. While key principles of data privacy addressed in the Directive remain largely the same, there are some significant policy changes, and, as a result, a fair amount of uncertainty about how the regulation will be enforced. With reports suggesting that many organizations won't be "fully compliant" by May 25, 2018 (the GDPR's enforcement date), the next year or two may prove instructive as the first round of enforcement begins.

Although some will find this uncertainty frustrating, there may be a silver lining. Where the Directive included an obligation to notify supervisory authorities about an organization's processing activities, the GDPR allows organizations to document their own processing activities, determine if they are compliant with the specific

JESSICA B. LEE *is a partner in the advanced media and technology practice at Loeb & Loeb.*

requirements, identify and mitigate any risks created by their data use, and ultimately hold themselves accountable for compliance. This emphasis on accountability and record keeping may actually help create the safety net needed to navigate the GDPR's grey areas. Organizations with a robust data governance program, that have a documented and considered approach to GDPR compliance, are much less likely to be at the front lines of GDPR enforcement, and certainly should not be subject to the highest fines (up to $20 million or 4 percent of global annual turnover).

GDPR: Accountability For Risk-Based Approach

Article 5(2) of the GDPR introduces the accountability principle, which requires organizations that control the processing of personal data ("controllers") to demonstrate (read: document) compliance with the GDPR's principles relating to the processing of personal data (i.e., lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality). This notion of accountability is not new; it was included as a basic data protection principle in the OECD Guidelines in 1980 (and the most recent update in 2013) and has been incorporated in various forms in other international privacy regulations. However, previous iterations of the accountability principle were centered on assigning responsibility or fault for failures in privacy compliance. Under the GDPR, accountability is recast as an obligation to establish a systematic and ongoing approach to privacy. In effect, it codifies the obligation to create a data governance program that incorporates the principle of privacy by design, using tools like privacy impact assessments to routinize data protection within an organization. More than just a mandate to create policy documents, the GDPR creates a regulatory environment under which privacy and data governance are forced to become a standard element of an organization's operations.

The GDPR replaces the previous Data Protection Directive 95/46/EC as the governing privacy regulation in the EU.

This principle of accountability must be viewed in the context of the GDPR's risk-based approach to privacy. Under Article 24 of the GDPR, controllers are required to assess the nature, scope, context and purpose of processing, and based on the risks presented: (1) implement appropriate technical and organizational measures to ensure and be able to demonstrate that data processing is performed in accordance with the GDPR; and (2) review and update those measures where necessary. Organizations are directed to take into account "the state of the art and the costs of implementation" and "the nature, scope, context, and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons." The GDPR provides suggestions (although no mandates) for which measures might be considered "appropriate to the risk." The pseudonymization and encryption of personal data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident, and the creation of a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing will provide a good start for organizations to start mapping out their compliance efforts.

DPIAs. Historically, national data protection authorities in Europe (DPAs) have recommended privacy impact assessments (PIAs), tools used to identify and mitigate privacy risks during the design-phase of a project, as an element of privacy by design. Under Article 35 of the GDPR, data protection impact assessments (DPIAs)—a more robust version of the PIA—are now mandatory when an organization is engaging in activities that pose a high risk to an individual's rights and freedoms. The DPIA presents an opportunity to demonstrate that safeguards have (hopefully) been integrated into an organization's data processing activities and that

the risks presented by a processing activity have been sufficiently mitigated

While the risks analysis itself is largely left in the hands of each organization, determinations that are wildly off-base may not be defensible. However, if an organization can justify its position, relying on industry practice or other guidance, even if regulators ultimately determine that additional measures were required, it may be able to avoid significant fines. Notably, the failure to complete a DPIA itself could result in fines of up to 10 million Euros or up to 2 percent of the total worldwide turnover of the preceding year.

Records of Processing. Under the Directive, organizations were obligated to notify and register processing activities with local DPAs. The GDPR eliminates this requirement and instead puts the burden on both controllers and processors to maintain an internal record of processing activities, which must be made available to DPAs upon request. These records must contain all of the following information: (1) the name and contact details of the controller and where applicable, the data protection office; (2) the purposes of the processing; (3) a description of the categories of data subjects and of the categories of personal data; (4) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations; (5) the transfers of personal data to a third country or an international organization, including the documentation of suitable safeguards; (6) the envisaged time limits for erasure of the different categories of data; and (7) a general description of the applied technical and organizational security measures. Where processing activities take place across a variety of disconnected business units, organizing these records may be challenging. Organizations will need to audit each of their business units and their corresponding systems and processes to determine their processing activities and consider moving to a more centralized system.

Next Steps: Preparing For May 25th and Beyond

Between now and May 25th, organizations should be focused on creating the processes and documents that will help tell the story of their GDPR compliance:

• Investigate and document the flow of data through your organization. Understand the sources of data the organization has control over, the systems or databases that data is stored in, the controls in place to protect that data, and how and when it's transmitted to third parties.

• Create records of processing and a process going forward for keeping those records up to date.

• Audit vendors and update agreements to include GDPR compliant provisions.

• Track the key requirements of the GDPR and document the data protection policies in place to address those obligations. Create a procedure for data breach response, data retention, and responding to data subject requests.

• Create a DPIA process—including a system to determine when a DPIA is needed and the team in charge of completion.

• Create a schedule and process to periodically audit the effectiveness of your data governance program.

• Conduct annual privacy training for employees.

While the process of preparing for the GDPR may be lengthy and expensive, it may ultimately give information security and internal data governance teams the resources needed to more effectively and strategically manage an organization's data. And, as the GDPR creates affirmative obligations for controllers to vet third party vendors for compliance with the GDPR's obligations, being able to demonstrate compliance with the GDPR through a strong data governance program won't just be a required regulatory obligation; it may be a selling point that distinguishes you as an organization that is safe to do business with.

General Data Protection Regulation

The Questions We'll Answer Today

- What Is the GDPR and Why Is Everyone Concerned About the Risks?
- How to Determine Whether the GDPR Applies to Your Business?
- How Will These New Rules Impact Your Ability to Engage in Data-Driven Advertising/Marketing?
- What You Should Be Doing Between Now and May 2018?

LOEB & LOEB LLP

What Is the General Data Protection Regulation (GDPR)?

- Europe's new framework for data protection
- Designed to harmonize data privacy laws across—it applies to ALL EU member states
- Expands current data protection requirements
  - Applies to all organizations that process the data of individuals in the EU
  - Expands the definition of personal information
  - Strengthens the data protection rights of individuals
- Includes security breach notification requirements for the first time
- Has no grandfather provision

Enforcement began on May 25, 2018

What Are the Risks Of Non-compliance?

- **Large Fines/ "Collective Redress"**
  Penalties for breaking the law can be up to 4% of a global enterprise's annual revenue
- **Administrative Oversight and Engagement**
  Data protection authorities can order changes to your practices, and can demand significant reporting obligations
- **PR Damage**
  Privacy is viewed as a fundamental right in Europe; violations are taken seriously
- **Business Relationships**
  Damage to relationships with partners and clients who may view it as risky to do business with you

LOEB & LOEB LLP

How to Determine If You're Within the Territorial Scope

Are you an EU company:

- applies to companies with an "establishment" in the EU

Are you a non-EU company that:

- *offers products and services* in Europe
- *processes personal data* from Europe
- *monitors behavior* of people in Europe

**the mere accessibility a website by individuals in the EU is insufficient.

** the use of a language or a currency generally used in one or more Member States in connection with ordering goods and services, or the mentioning of customers or users who are in the EU will indicate an intent to offer products/services in the EU.

LOEB & LOEB LLP

Do You Process Personal Data?

Processing

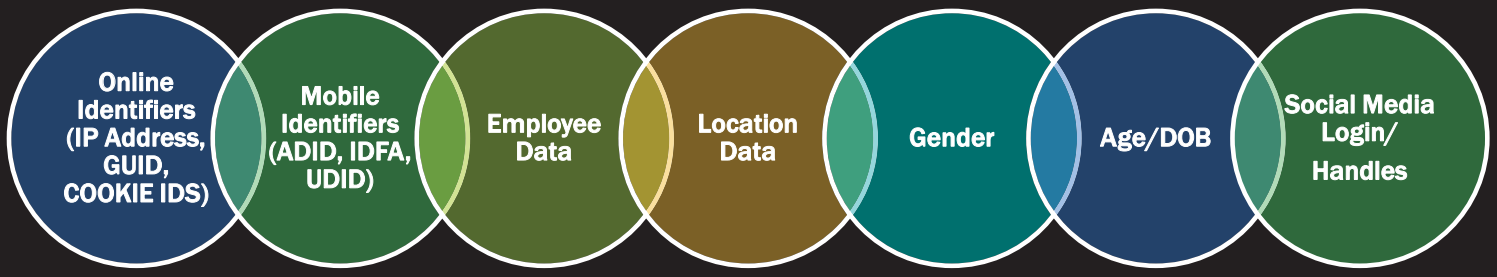
Includes: collection, recording, organizing, structuring, storing, adapting, altering, retrieving, consulting, using, disclosure, transmission, and erasure

Personal Data

Includes: any information relating to an identified or identifiable natural person (“data subject”); includes name and address, but also location, online identifiers, social identity, description, image, and IP address

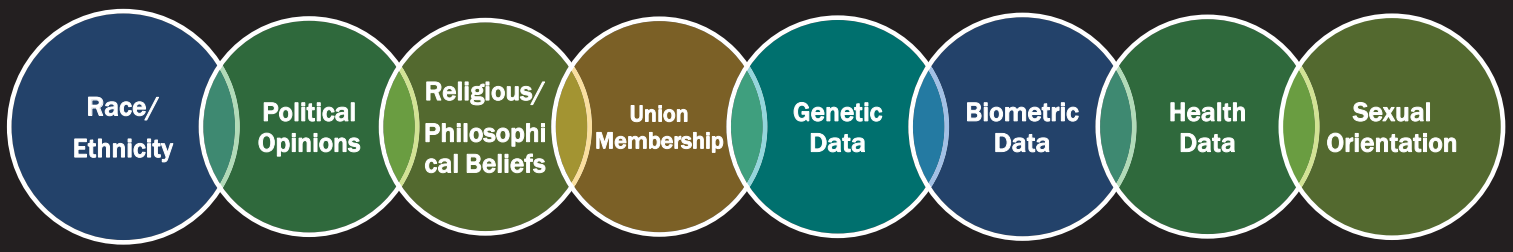
LOEB & LOEB LLP

Personal Data Is More Than Name, Email or Phone Numbers...



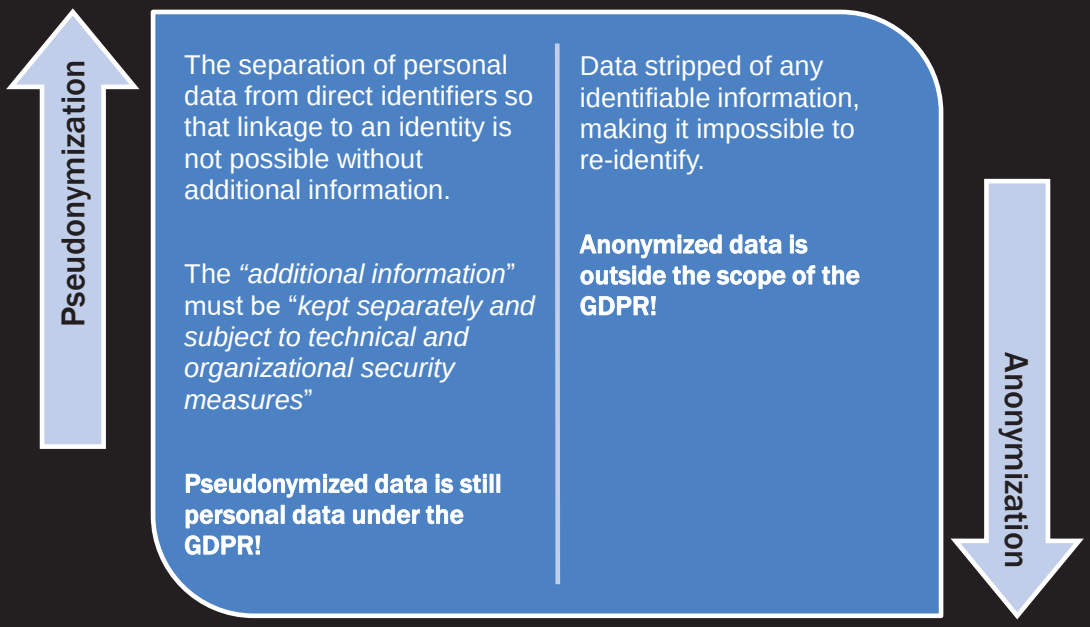
LOEB & LOEB LLP

Special/Sensitive Categories of Data Requires Special Treatment (Explicit Consent)



LOEB & LOEB LLP

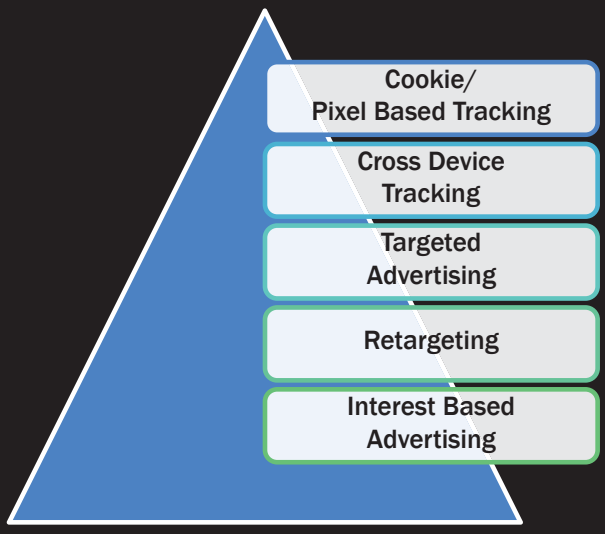
Can You Rely on "Anonymization"? Only If the Data Is Truly "Anonymized"



Consider this: With only a few data points, it may be possible to identify a data subject, even without their name or home address.

LOEB & LOEB LLP

Are You Engaging in Any Of These Activities? If So, You May Be "Monitoring"



Data Protection Officers

- Some organizations must appoint a data protection officer (DPO)
- When to appoint a DPO:
  - Systematically monitor large groups of individuals
  - Carry out large-scale processing of special categories of data, including data related to criminal convictions and offences
- DPO responsibilities:
  - Actively monitor compliance with the GDPR
  - Provide advice on data impact assessments
  - Remain independent and report to “highest management level”

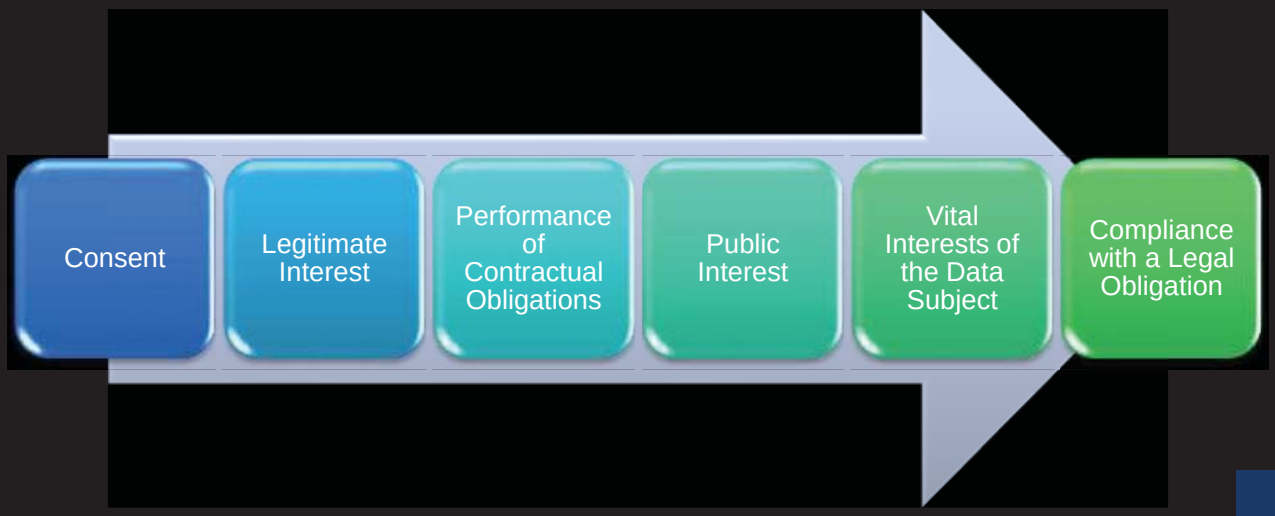
Data Breach Notification

- **Breach Notification**
  - Notification to supervisory authority “without undue delay”
  - And, where feasible, not later than **72 hours** after becoming aware of the breach.
  - Notification to consumers in high risk situations

How Will These Rules Impact Your Data-driven Business?

Understand whether you have a lawful basis to process personal information

Under the GDPR, a Company Must Have a "Lawful Basis" to Process Personal Information



LOEB & LOEB LLP

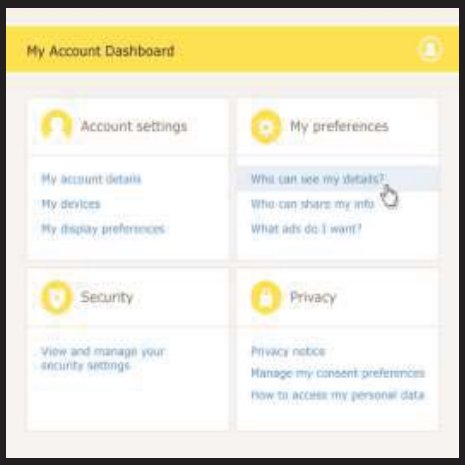
GDPR Mandates Affirmative Consent

Unambiguous	Freely Given Consent is not freely given if:	Informed	Specific Consent must relate to specific processing operations:	Explicit Required for:
•A statement or clear affirmative action •Silence, pre-ticked boxes and inactivity, will not constitute consent	• The data subject has no genuine and free choice or is unable to refuse or withdraw consent without consequence • The performance of a contract is made conditional on the data subject's consent • Bundled with other consents	•Data subjects should understand the extent to which they are consenting and be aware, at least, of the identity of the controller and the purposes of the relevant processing	• A general broad consent to unspecified processing operations will be invalid • If data processing has multiple purposes, a consent should cover all those purposes	•Sensitive data •Profiling activities •Cross-border data transfers

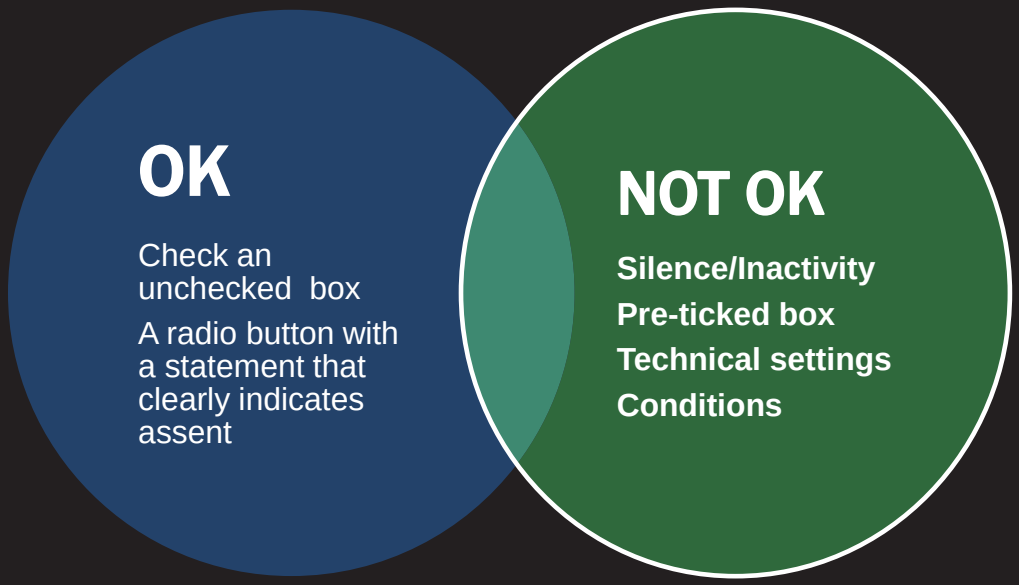
LOEB & LOEB L_P

What Does Unambiguous Consent Look Like?

- Signing a consent statement on a paper form
- Ticking box
- Selecting from equally prominent yes/no options
- Choosing technical settings or preference dashboard settings
- Responding to an email requesting consent
- Volunteering optional information for a specific purpose



Explicit Consent Requires a Direction Action



Checklist for Consent

- ☐ Is consent the most appropriate lawful basis for processing?
- ☐ Is the request for consent prominent and separate from the terms and conditions?
- ☐ Is consent given on an "opt-in" basis? (i.e. no pre-ticked boxes or consent by default)
- ☐ Is the consent written in clear, plain language that is easy to understand?
- ☐ Does the consent specify the scope of what is being collected and how it will be used?
- ☐ Is the individual given options to consent to independent processing operations? (e.g. emails, targeted ads, sharing with third parties)
- ☐ Do we provide the name of the company and any third party controllers who will be relying on the consent?
- ☐ Do we tell individuals they can withdraw their consent?
- ☐ Do we ensure that the individual can refuse to consent without detriment?
- ☐ Consent is not a precondition of a service.

LOEB & LOEB LLP

Consent has limitations

- Consent can be revoked
  - Data subjects must be informed in advance that they can change their minds
  - Once consent is withdrawn, data subjects may ask to have their personal data erased and no longer used for processing.

- Consent is limited to the purpose for which it was collected
  - Consent for subsequent processing may not be required if the operations are “compatible”

  - Compatibility depends on:
    - ✓ the link between the processing purposes
    - ✓ the reasonable expectations of the data subject
    - ✓ the nature and consequences of further processing
    - ✓ the existence of appropriate safeguards for the data

- Must be able to demonstrate consent was obtained in compliance with the GDPR

- → Any consent already in place needs to be reviewed to meet GDPR standards

LOEB & LOEB LLP

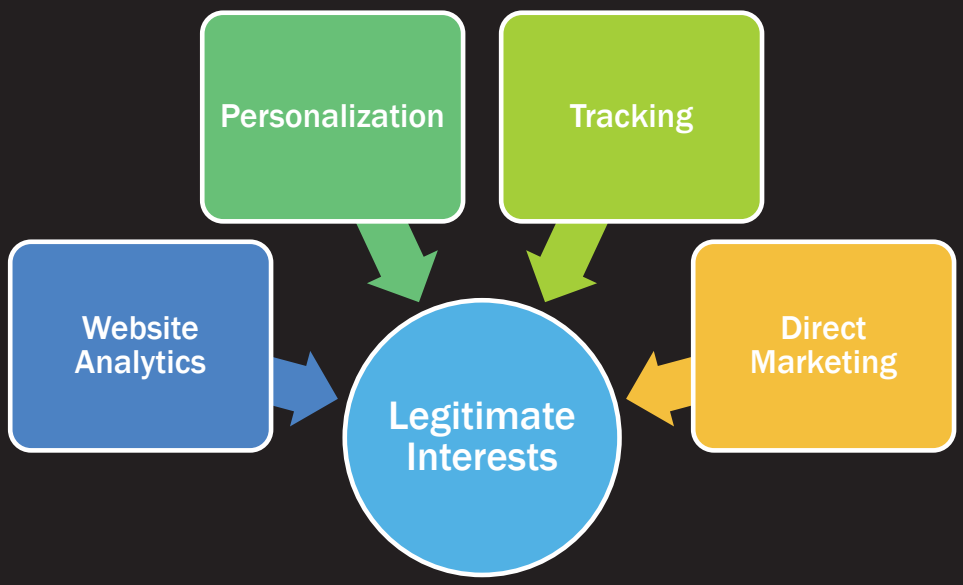
If Consent Isn't Available, Consider Whether You Can Establish a Legitimate Interest

Legitimate Interest – 3 Part Test

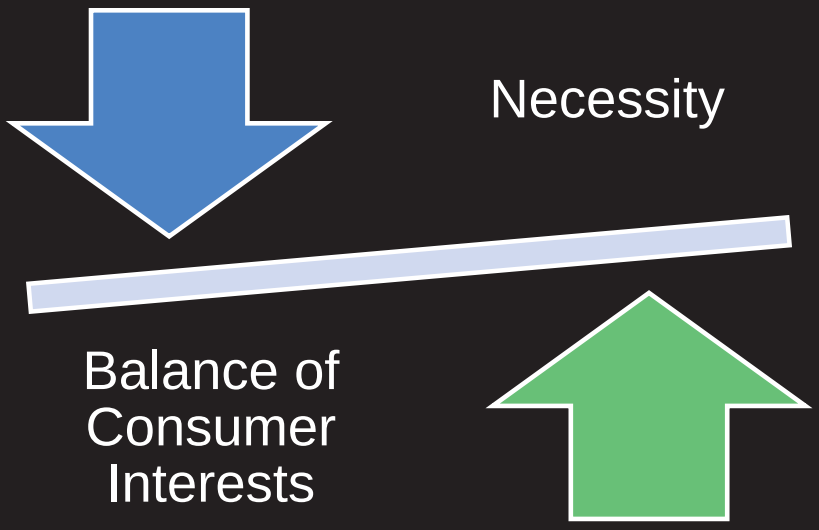
- Identify the legitimate interest
  - Is it required to achieve a lawful business objective?
  - Consider all possible uses (including third party processing)
- Is it "necessary" ?
  - Be able to articulate why there is no other way to achieve the objective (or if alternative means would require disproportionate effort)
  - This may require a privacy impact assessment
- Balance your need against the consumer's interests
  - The rights and freedoms of the individual should not override the Legitimate Interest.

** *Legitimate Interests can be those of the Controller or a Third Party. A number of parties may have a Legitimate Interest in processing the Personal Data.*

These May Be Legitimate Interests



Do the Privacy Rights of The Data Subject Override the Need for the Processing?



Consider:

- ✓ The reasonable expectations of the individual
- ✓ The type of data (i.e. is additional protection required?)
- ✓ The benefit to the consumer
- ✓ The impact of processing
- ✓ Any safeguards which are or could be put in place

LOEB & LOEB LLP

What Rights Do "Data Subjects" Have?

Right to Be Informed	• The data subject should be informed about what information is being collected, how it will be used, and the consequences of that use. The data subject should also be informed about the right to object or to request access, rectification or the erasure of the data (where applicable)
Right to Object	• The data subject has the right to object or withdraw consent to processing (including targeting/profiling) and avoid profiling-based decisions.
Right to Access	• The data subject has the right to obtain confirmation about what personal data a controller has and how it is being used, including whether it is being used for automated decision-making, and who it has been shared with. A data subject has a right to a copy of his/her data.
Right to Erasure/ Rectifi-cation	• If the basis for profiling is consent and consent is withdrawn, controllers must erase the relevant personal data, unless there is another legal basis for the profiling. If the data is inaccurate, data subjects have the right to request that it is rectified

What Other Principles Apply?

Purpose Limitation

- Data must be collected for specified and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- Compatibility of purposes depends on:
  - the relationship between the purposes
  - the context of the collection & reasonable expectations of the data subject
  - the nature of the data and the impact of the further processing
  - safeguards applied by the controller to ensure fair processing

Data Minimization

- Data minimization refers to the practice of limiting the collection of personal information to that which is directly relevant and necessary to accomplish a specified purpose
- Don't collect data because "it might be useful in the future"
- Consider whether data can be anonymized for continued use

Memory Limitation

- Data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Onboarding, Processing and Sharing Personal Information

Applying the Principles of the GDPR

What to Ask When Onboarding Data

- What type of data will you receive? (personal? sensitive? pseudonymized?)
- What consent was obtained when the data was initially collected?
- Can the data be used in the way you need to use it?
- What are the use cases, have those been clearly specified?
- Can the data be appended, merged, combined or aggregated with other data sets?
- Do you have promises/guarantees (reps and warranties) about the data ?

LOEB & LOEB LLP

Processing Data: Special Rules For “Profiling”

What is profiling under the GDPR?

- Automated processing of personal data to evaluate certain personal aspects relating to a natural person
- Specific examples include: analyzing or predicting a person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements

PROFILING  **TRACKING**

- Profiling is the intention to ***make decisions*** regarding a data subject or ***analyze/predict*** the subject’s behaviors and preferences.

LOEB & LOEB LLP

Which of These Could Be Considered Profiling?

- CONTEXTUAL ADVERTISING ☒
- BEHAVIORAL RETARGETING ☑
- CREATING AUDIENCE SEGMENTS ☑
- INTEREST BASED ADVERTISING ☑

LOEB & LOEB LLP

Special Rules for Automated Decision Making

Automated decision-making is the ability to make decisions by technological means without human involvement

•Prohibited (with exceptions) if it has a "Significant" or "Legal Effect"

Legal effects

- Has an impact on legal rights
- Affects a person's legal status
- Affects rights under a contract

Significant affects

- Must be more than trivial
- Must have the potential to significantly influence the circumstances, behavior or choices of individual
- Leads to discrimination

Examples: Automatic refusal of an on-line credit application or e-recruiting practices without any human intervention.

LOEB & LOEB LLP

Data Subjects Have a Right Not to Be Subject to Automated Decision-making ("ADM"), Unless…

- These Exceptions Apply:

- ADM is necessary to enter a contract
- Explicit consent is given
- Authorized by Union or member state law, which includes suitable safeguards

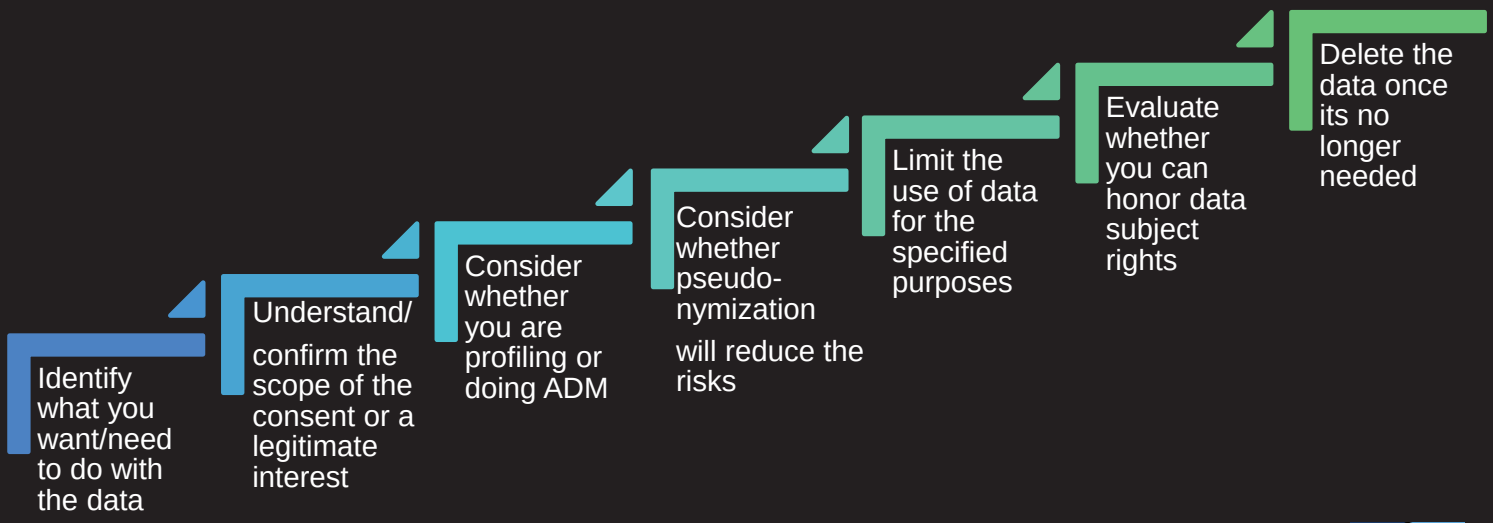
→ Safeguards MAY include anonymization or pseudonymization

Consider:

- The intrusiveness of the profiling
- The expectations of the data subject
- The right to challenge the decision

LOEB & LOEB LLP

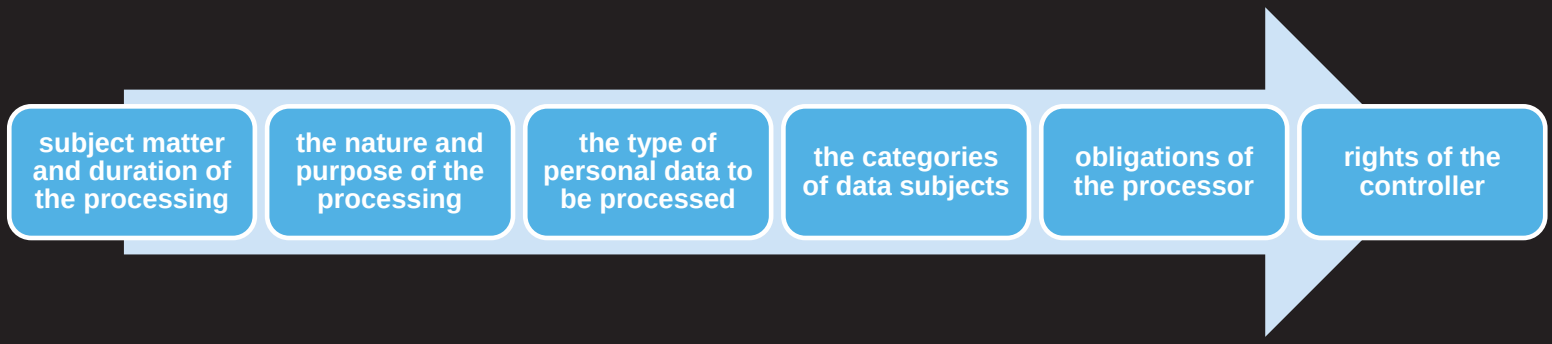
Consider These Steps Prior to Processing



What to Consider Before Sharing Data

- What is the scope of your consent/legitimate interests?
- What will the third party do with that data - is any additional processing by the third party "compatible" with the original consent?
- Has the third party's security protocols been vetted?
- Can/will the third party help you honor data subject rights and comply with your security breach notification obligations?

Sharing Data: Points to Address in a Data Processing Agreement

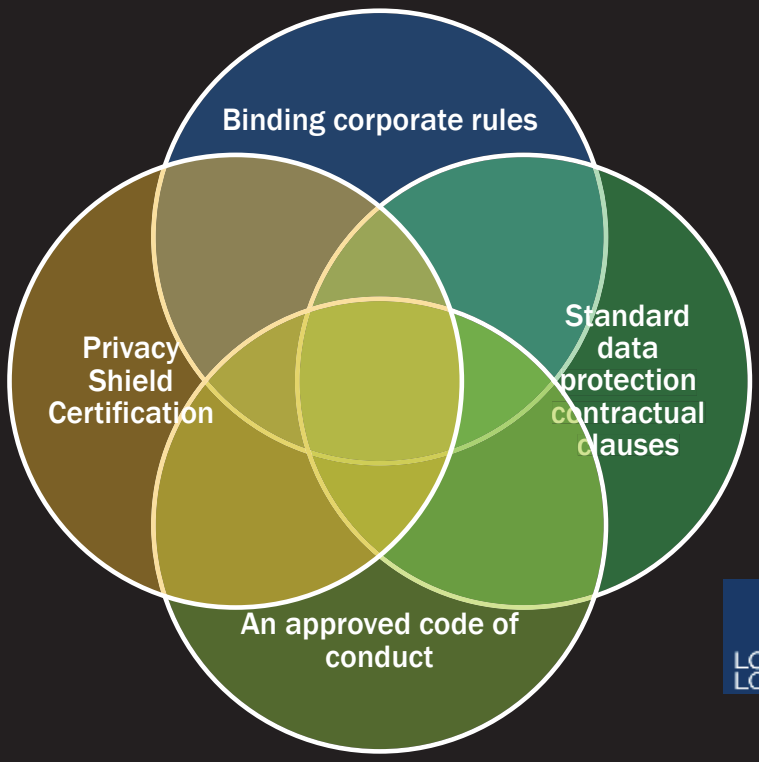


Vendor Due Diligence: Key Questions to Ask

- Where is the vendor based? Where will the data be held and accessed?
- Will the vendor act as a processor or controller?
- Does the vendor use the data to pursue its own interests?
- Will the vendor be using any subcontractors? If so, where are they based?
- What are the technical & organizational security measures the vendor uses to protect data?
- What are their policies / procedures / certifications to protect data? Are these good enough?
- Does the vendor comply with a code of conduct on how it uses data?
- Does the vendor have a privacy seal?
- Can the vendor assist in honoring data subject rights?

Special Mechanisms Are Needed to Transfer Data Outside of the EU

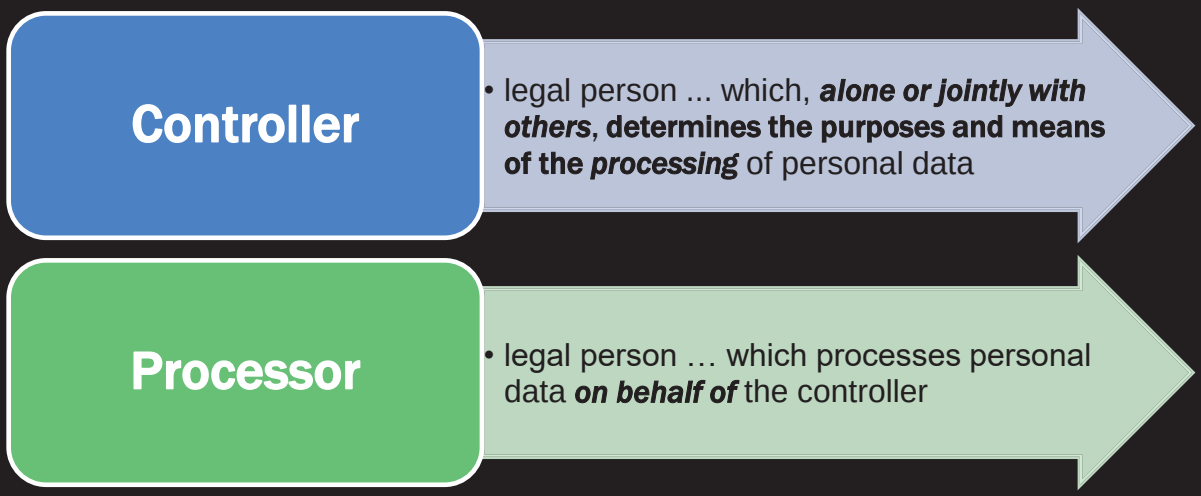
There are a handful of approved mechanisms:



LOEB & LOEB LLP

What Will You Need to Do?

Understand Your Role and Obligations



Controllers Vs. Processors

Controllers	Processors
Comply with the GDPR principles relating to processing of personal data.	Maintain a record of all processing operations under their responsibility
Honor data subject rights	May be a joint controller for data processing beyond the scope of the controller's instructions
Implement technical & organizational measures to protect personal data	Directly responsible for implementing appropriate security measures
Enter into written agreements with processors requiring security obligations	Must inform a controller immediately of any data breach

How to Determine Your Role

Consider:

- How did you obtain the data? Is it first, second or third party data?
- Do you determine the techniques used for processing (cookie syncing, data matching)?
- If you are a third party, do you incorporate the data into your own products or services?

Depending on the control you have over the data, you may be a controller, a processor or a joint controller – this determination is based on your activities, it cannot be determined by contract

LOEB & LOEB LLP

Consider the Responsibilities/Obligations

As processors:

- You can only process data as permitted by controller agreements
- You will need prior consent to engage vendors ("sub-processors")

As controllers, you have more control, but:

- You may have direct responsibility for honoring data subject rights
- You have more detailed record keeping obligations
- You are directly responsible for security breach notification obligations

**Joint-controllers will need to allocate responsibilities via contracts

“Accountability” Documenting Your Compliance

- **Maintain Records of Processing**

- **Conduct Privacy Impact Assessments**
  - May be conducted on a routine basis to help keep records up to date when collecting new information or sharing with a third party

- **Conduct Data Privacy Impact Assessment**
  - A mandatory operation for high risk processing
  - Examples of when a DPIA is needed
    - Profiling
    - Engaging in automated decision making with significant or legal effect
    - Large scale data processing
    - Processing that will prevent data subjects for exercising a right

“Accountability” Documenting Your Compliance

You must “implement appropriate technical and organizational measures” that are “appropriate to the risk”

Consider:

- Pseudonymization and encryption of personal data
- Access controls
- Back-up/contingency plan that will ensure the ongoing confidentiality, integrity, and availability of your systems
- A process for regularly testing, assessing and evaluating the effectiveness of your security measures

Record keeping obligations: controllers

Records must contain the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
- the purposes of the processing
- a description of the categories of data subjects and the categories of personal data being processed
- the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries
- where applicable, an indication of any transfers of personal data to a third country, including the name of the third country, and the documentation of suitable safeguards (if applicable)
- where possible, the time limits for erasure of the various categories of data being processed
- where possible, a general description of the applicable technical and organizational security measures

Record keeping obligations: processors

Records must contain the following information:

- the name and contact details of the processor or processors and of each controller on whose behalf the processor is acting and, where applicable, the controller's or processor's representative as well as the data protection officer
- the categories of processing carried out on behalf of each controller
- where applicable, an indication of any transfers of personal data to a third country, including the name of the third country, and the documentation of suitable safeguards (if applicable)
- where possible, a general description of the technical and organizational security measures taken to protect the personal data

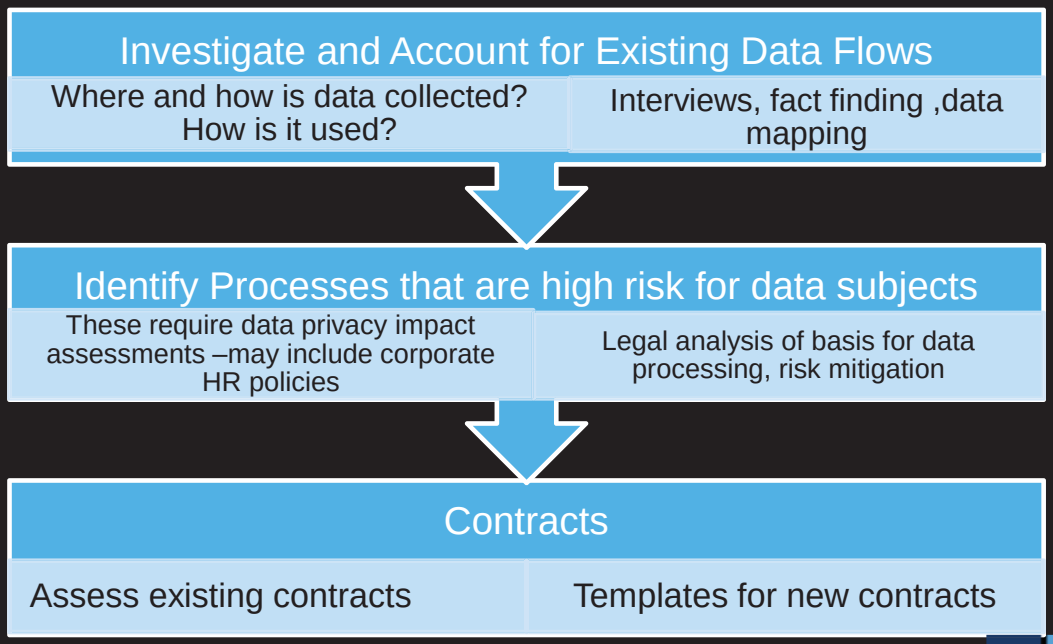
Next Steps in GDPR Readiness

Preparations for GDPR

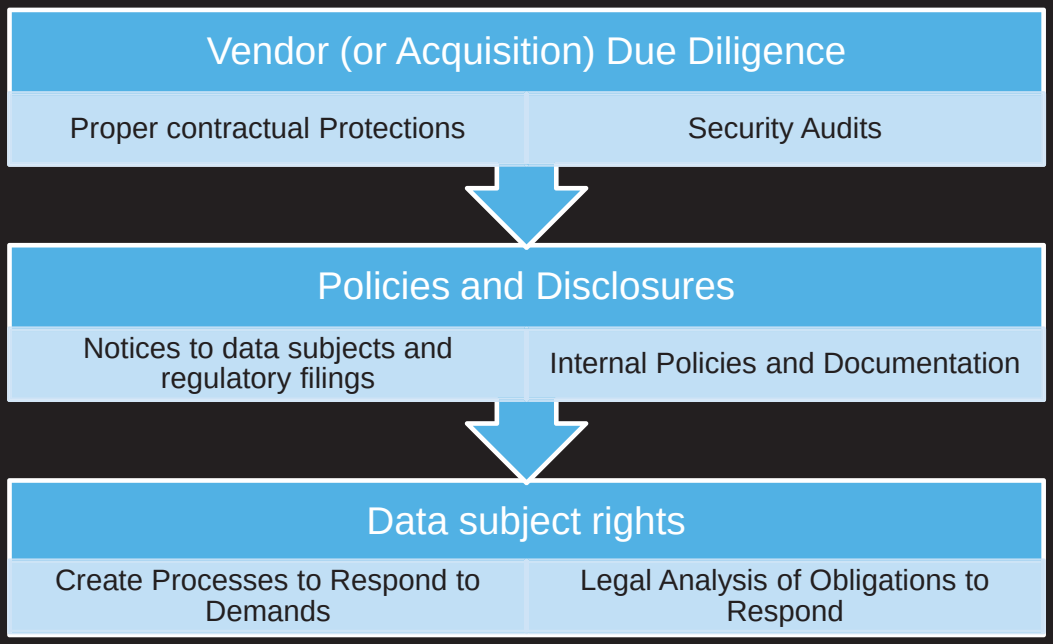
- **Create Framework** for ongoing compliance and data governance
- **Advise on selection of DPO** and support organization
- **Review existing data management** and identify gaps
- **Opportunity for ongoing support** of company's data governance and corporate governance

LOEB & LOEB LLP

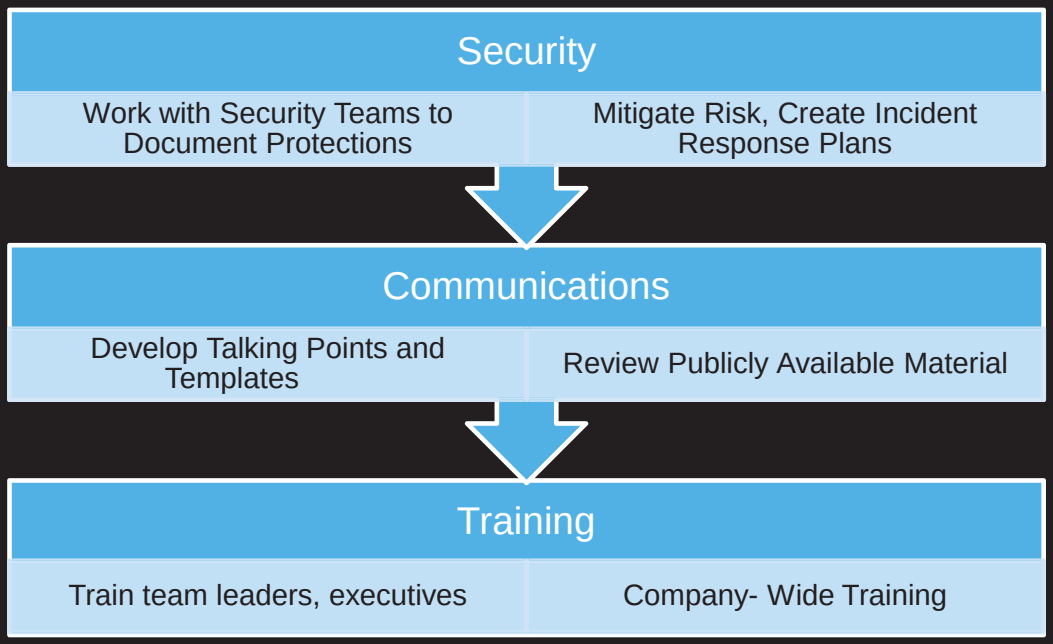
How do we support preparations for GDPR?



Preparations for GDPR



Preparations for GDPR



What to Do Between Now and May 2018

- Investigate & understand the flow of data through your company
  - What do you collect/receive? What do you do with it? Where do you send it/when do you delete it?
- Complete Records of Processing
- Complete a gap assessment
- Review & update contracts (if needed)
- Review & update consents/privacy notices (if needed)
- Create a Security Breach Notification process.
- Complete PIA/DPIA for ADM/Profiling/Processing based on Legitimate Interests

What to Look for in the Next Few Months

- Codes of Conduct
- Member State Guidance
- Industry Specific Guidance

Questions?

Jessica B. Lee
jblee@loeb.com
https://www.loeb.com/attorney-jessicablee

Internet of Things
Update

NYSBA

CONNECTED DEVICES

IoT devices will go from 2 billion in 2006 to 200 billion in 2020

That's about **26** devices per person

The number of smart home devices will grow from **42** million **TO** **244** million within five years

Today's IoT Landscape

Things Move Fast…

L.L. Bean says it might offer discounts for clothing that tracks your habits

Dennis Green
Feb. 7, 2018, 4:48 PM 5,460

L.L. Bean To Continually Track Clothing After Purchase

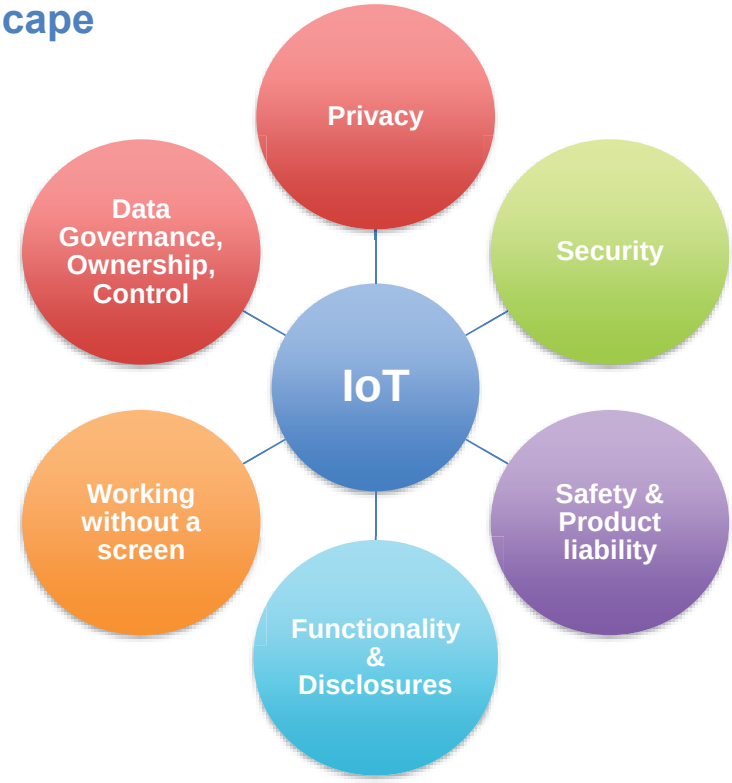
by **Chuck Martin** , Staff Writer, February 9, 2018

L.L. Bean Backs Off Of Continually Tracking Clothing After Purchase

by **Chuck Martin** , Staff Writer, February 10, 2018

Today's IoT Landscape

Key Issues



NYSBA

Privacy

NYSBA

FEDERAL TRADE COMMISSION

PROTECTING AMERICA'S CONSUMERS

- **Updated COPPA Guidance** (June 2017)
  - Connected toys and devices, voice-activated tech
  - New methods of parental consent (including facial recognition)
- **Enforcement Policy Statement** (October 2017)
- **Workshop on Informational Injury** (December 2017)

v vtech

January 2018: Connected toy app alleged to have collected children's info without parental consent

- Didn't link to privacy policy everywhere info was collected
- Didn't provide direct notice of collection
- Failed to protect information (intrusion prevention or detection)
- Failed to encrypt as stated in privacy policy
  - → Alleged violations of COPPA, FTC Act
  - → $650,000 settlement

Consumer Product Safety Commission

The CPSC held a hearing focused on IoT product safety but limited the scope of its inquiry to **physical injury** (explicitly excluding data and privacy concerns from its analysis).

The FTC filed comments, and identified 3 security practices it thinks the CPSC should focus on to counter consumer hazards:

- **Risk assessment** – test authentication techniques and communication
- **Vendor oversight, interdependent products** – conduct due diligence with vendors, incorporate security standards in contracts, verify compliance
- **Software updates, "expiration dates" and default settings** – take a holistic view of the marketplace and stay up to date on new trends; consider patch vulnerabilities and security-only updates

NTIA to Update U.S. Privacy Laws

- Senate Committee on Commerce, Science & Technology holds hearing in November 2017 to discuss privacy and security threats to U.S. consumers.
- Industry groups urge Congress and NTIA to better protect consumers and propose consumer protects to ensure routine security devices for IoT devices and carefully assess IoT when used for “critical functions” such as transportation, home security or medical devices.

STATES ARE ALSO POLICING PRIVACY

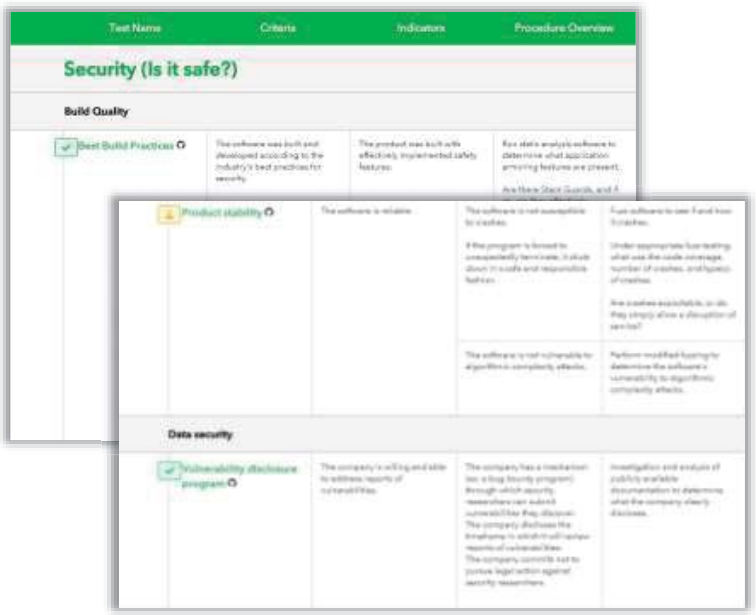
NYSBA

Security

FTC Warns Device Makers on Security
February 2018

- “Start with security” (repeated from June 2015)
- Streamline the update process for consumers
- More and better information about security update support

Consumer Reports – The Digital Standard



Some criteria is still under review:

: Well understood with a developed testing approach in place.

: Under development with some outstanding questions.

: Under discussion, usually due to the sensitivity and complexity of the issue.

Consumer Reports – Updates

- Consumer Reports conducted their first review using the Digital Standard to rate connected TVs
- Findings revealed overly-broad data collection, security flaws and privacy concerns
- More review of consumer products to come
- Recently introduced new ratings criteria to the Digital Standard (data privacy and security) to measure peer-to-peer payments
- Reviewed P2P payment services including Apple Pay, Facebook Payments (in Messenger), Square's Cash App, Venmo and Zelle

Consumer Reports – Smart TVs

February 2018

- Consumer Reports reviewed 5 different smart TVs (Samsung, TCL, LG, Sony and Vizio)
- Found all used automatic content recognition (ACR)
- Discovered security vulnerabilities on some models that allowed outside attacker to control TV functions
- Some features and data collection could be disabled but severely limited the functioning of TV
- Other categories to come soon!

Consumer Reports – Peer-to-Peer Payments
June 2018

MOBILE PEER-TO-PEER PAYMENT SERVICES						
SERVICE	OVERALL SCORE	PAYMENT AUTHENTICATION	DATA SECURITY	DATA PRIVACY	CUSTOMER SUPPORT	BROAD ACCESS
Apple Pay	76	⏫	🔼	⏫	🔼	❗
Venmo	69	🔼	❗	🔽	⏫	⏫
Cash App (Square)	64	❗	🔼	🔽	🔼	⏫
Facebook P2P Payments in Messenger	63	🔼	🔼	🔽	🔽	⏫
Zelle (standalone app)	50	❗	🔽	🔽	⏫	❗

NYSBA

LOEB & LOEB LLP

Security Concerns

- Constant data collection
- Unexpected uses of consumer data
- Unencrypted data (especially at rest)
- Device and network authentication
- Representations about security can create liability

How long do IoT devices last?

What do consumers expect?

Grace v. Apple

Apple created an alternative version of FaceTime for iOS 7, and in April 2014 disabled FaceTime on iOS 6 and earlier versions. Users with earlier model phones/iOS sued Apple for their inability to use FaceTime.

- In July 2017, judge rules that iPhone 4 and 4S users can pursue nationwide class action claims that Apple intentionally “broke” FaceTime (to save money from routing calls through servers owned by a third party).
- As of August 2018, the parties are undergoing discovery, obtaining expert testimony and fighting over class certification. Expert discovery (including depositions) are scheduled to be completed by September 27, 2018.

Discontinuations and Product Lifecyle

- **Robot Kuri** – In July 2018, Mayfield Robotics (an entity of the Bosch Startup Platform) announced that it is pausing operations of its Robot Kuri, a “home” robot that launched at CES in 2017. Mayfield will stop manufacturing, will not ship robots out to customers and will refund all pre-order deposits.
- **Amazon “Mayday” Button** – In June 2018, Amazon announced that it will immediately discontinue the “Mayday” button which allows customers to summon face-to-face customer service on their Amazon Fire rather than calling the Amazon Customer Service Line.

Discontinuations and Product Lifecyle

- **Logitech Harmony Link** – In November 2017, Logitech announced that it will be discontinuing service for the Harmony Link remote system. The device and its cloud-based system allow users to control home theater and sound equipment from a mobile app. Customers received an e-mail explaining that Logitech will "discontinue service and support" for the Harmony Link as of March 2018, adding that Harmony Link devices "will no longer function after this date." Effectively, Logitech's decision has "bricked" the smart remote device.
- **Intel** – In June 2017, Intel announces it will discontinue the Galileo, Edison, and Joule computer products by posting notices on their website that the company will no longer support the product lines.

ADA Compliance

- January 2018 – new federal regulations took effect (requiring all federal websites comply with the ADA).
- Title III of the American with Disabilities Act regulates private sector businesses. “Business to consumer” websites should comply with the ADA.
- ADA includes minimum requirements for websites like being fully navigable via keyboard and/or screen reader software, text contrast, text scaling, etc.

Questions?

Thank you!

Before the
CONSUMER PRODUCT SAFETY COMMISSION
Washington, DC

In the Matter of The Internet of Things and Consumer Product Hazards	Docket No. CPSC-2018-007

To: Consumer Product Safety Commission
Date: June 15, 2018

Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection

I. Introduction

The staff of the Federal Trade Commission's ("FTC") Bureau of Consumer Protection ("BCP") (hereafter "BCP staff') appreciate this opportunity to comment[1] on the Consumer Product Safety Commission's ("CPSC") Notice of Public Hearing and Request for Written Comments ("RFC") on *The Internet of Things and Consumer Product Hazards.*[2] Among other things, the RFC seeks comment on existing Internet of Things ("IoT") safety standards, how to prevent hazards related to IoT devices, and the role of government in the effort to promote IoT safety.

The market for Internet-connected devices—ranging from light bulbs to smart TVs to wearable fitness trackers—is flourishing. The rapid proliferation of such devices in recent years has been truly remarkable, with an estimated 8.4 billion IoT devices in use in 2017—a 31% increase from 2016.[3] And this trend promises to continue: it is estimated that 55 billion IoT devices will be installed around the world by 2025.[4]

This burgeoning marketplace offers enormous benefits to consumers—including many products that offer safety benefits.[5] For example, IoT medical devices track health data that

[1] These comments represent the views of the staff of the Bureau of Consumer Protection. The Commission has voted to authorize BCP staff to submit these comments.
[2] 83 Fed. Reg. 13122 (Mar. 27, 2018).
[3] *Gartner Says 8.4. Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016*, GARTNER (Feb. 7, 2017), https://www.gartner.com/newsroom/id/3598917.
[4] Peter Newman, *The Internet of Things 2018 Report: How the IoT is Evolving to Reach the Mainstream with Businesses and Consumers*, BUS. INSIDER INTELLIGENCE (Feb. 26, 2018), http://www.businessinsider.com/the-internet-of-things-2017-report-2018-2-26-1.
[5] *See generally* FED. TRADE COMM'N, FTC STAFF REPORT: INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, 7-10 (Jan. 2015) [hereinafter FTC IOT REPORT], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-

informs patients' diagnosis and treatment.[6] Connected cars offer both safety and convenience benefits, such as real-time notifications of dangerous conditions and smartphone starter and sound-system control.[7] And home IoT devices called "water bugs" detect flooding in basements, while other devices monitor energy use, identify maintenance issues, and remotely control devices such as lights, ovens, and wine cellars.[8] Consumers also may purchase devices such as Internet-connected locks, burglar alarms, cameras, and garage doors for their physical safety.

But such benefits may be foreclosed if IoT devices themselves are a hazard. Like any other consumer product, IoT products might present hazards such as fires and burns, shock, and chemical exposure. IoT devices might also create additional technology-related hazards associated with the loss of a critical safety function, loss of connectivity, or degradation of data integrity.[9] For example, a car's braking systems might fail when infected with malware,[10] carbon monoxide detectors or fire alarms might stop working with the loss of connectivity,[11] and corrupted or inaccurate data on a medical device might pose health risks to a user of the device.[12] Consumers' physical safety could also be at risk if an intruder had access to a connected lock, garage door, or burglar alarm.

Requiring IoT devices to have perfect security would deter the development of devices that provide consumers with the safety and other benefits discussed above.[13] Conversely, insecure devices can erode consumer trust if consumers cannot rely on the safety and security of

---

workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing benefits of the IoT) (Commissioner Wright dissenting and Commissioner Ohlhausen issuing a concurring statement).

[6] *Id.* at 7-8.

[7] *Id.* at 9.

[8] *Id.* at i and 8-9.

[9] CONSUMER PROD. SAFETY COMM'N, POTENTIAL HAZARDS ASSOCIATED WITH EMERGING AND FUTURE TECHNOLOGIES, 16 (Jan. 18, 2017) [hereinafter CPSC EMERGING TECHNOLOGIES REPORT], https://www.cpsc.gov/content/potential-hazards-associated-with-emerging-and-future-technologies (citing potentially new consumer product hazards related to IoT, including loss of safety function, loss of connectivity, and issues related to data integrity).

[10] *See, e.g.*, Jeff Plungis, *Your Car Could Be The Next Ransomware Target*, CONSUMER REPORTS (June 01, 2017), https://www.consumerreports.org/hacking/your-car-could-be-the-next-ransomware-target/. *See also* Catalin Cimpanu, *Volkswagen and Audi Cars Vulnerable to Remote Hacking*, BLEEPINGCOMPUTER (April 30, 2018), https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/ and Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4 M Vehicles For Bug Fix*, WIRED (July 24, 2015), https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[11] *Cf.* Richard Speed, *Three-Hour Outage Renders Nest-Equipped Smart Homes Very Dumb*, THE REGISTER (May 17, 2018), https://www.theregister.co.uk/2018/05/17/nest_outage/ (reporting that an outage in the Nest system left consumers "unable to arm/disarm or lock/unlock" their homes remotely, leaving frustrated consumers to set their alarms and lock their doors manually).

[12] Shaun Sutner, *FDA and UL weigh in on security of medical devices, IoT*, IOT AGENDA, https://internetofthingsagenda.techtarget.com/feature/FDA-and-UL-weigh-in-on-security-of-medical-devices-IoT.

[13] The FTC does not expect perfect security. *See e.g.* Prepared Statement of the Fed. Trade Comm'n, *Protecting Consumer Information: Can Data Breaches be Prevented? Before the Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, U.S. House of Representatives*, 4 (Feb. 5, 2014), https://energycommerce.house.gov/hearings/protecting-consumer-information-can-data-breaches-be-prevented/ ("[T]he Commission has made clear that it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.")

their device.[14] Companies that manufacture and sell IoT devices must take *reasonable* steps to secure them from unauthorized access. Poorly-secured IoT devices create opportunities for attackers to assume device control, opening up risks that may include safety hazards.[15] For example, hackers used the Mirai botnet—composed of IoT devices, such as IP cameras and routers, infected with malicious software—to engage in a distributed denial of service ("DDoS") attack of unprotected residential building management systems in Finland. By blocking Internet access, hackers sent these connected management systems into an endless cycle of rebooting, leaving apartment residents with no central heating in the middle of winter.[16] Also, earlier this year, researchers discovered vulnerabilities in Internet-connected gas station pumps that, when remotely accessed, would allow hackers not only to steal credit card information but also change the temperature and pressure in gas tanks, potentially causing explosions.[17]

Although the request for comment specifically notes that the CPSC "will not address personal data security or privacy implications of IoT devices," security risks associated with IoT devices may implicate broader safety concerns, not just privacy. For example, a criminal who hacks into a connected-home network could not only collect information about consumers who live in the house, but also could activate or deactivate home security devices, potentially causing threats to personal safety.[18] A company setting up a program to address security risks on its IoT device should take measures to secure that device from hackers, for both privacy *and* safety issues. Through this comment, BCP staff shares some of its expertise in promoting IoT device security, and makes certain recommendations to the CPSC. The recommendations focus on three issues: (1) best practices for predicting and mitigating against security hazards; (2) the process for encouraging consumers to register for safety alerts and recall information; and (3) the role of government in IoT security.

II. Background on the FTC

The FTC is an independent administrative agency responsible for protecting consumers and promoting competition. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect consumers' privacy and security. The primary law enforced by the FTC, the FTC Act, prohibits unfair and deceptive acts or practices in or affecting commerce,

---

[14] *See e.g.* FED. TRADE COMM'N, MOBILE SECURITY UPDATES: UNDERSTANDING THE ISSUES, 1 (Feb. 2018) [hereinafter "MOBILE SECURITY REPORT"], https://www.ftc.gov/reports/mobile-security-updates-understanding-issues; FTC IOT REPORT at 20-21; and Comments of the Staff of the Fed. Trade Comm'n, *In the Matter of Communicating IoT Device Security Update Capability to Improve Transparency for Consumers*, Nat. Telecomm. Info. Admin. (June 19, 2017), https://www.ftc.gov/policy/advocacy/advocacy-filings/2017/06/ftc-comment-national-telecommunications-information.

[15] *Id. See also* Chris Morris, *465,000 Pacemakers Recalled on Hacking Fears*, FORTUNE (Aug. 31, 2017), http://fortune.com/2017/08/31/pacemaker-recall-fda/; and Lisa Vaas, *350,000 Cardiac Devices Need a Security Patch*, NAKED SECURITY (May 4, 2018), https://nakedsecurity.sophos.com/2018/05/04/half-a-million-pacemakers-need-a-security-patch/.

[16] Richard Chirgwin, *Finns Chilling as DDoS Knocks Out Building Control System*, THE REGISTER (Nov. 9, 2016), https://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/.

[17] Alfred Ng, *Hackers Should Be Pumped About Gas Station Security Flaws*, CNET (Mar. 12, 2018), https://www.cnet.com/news/gas-stations-online-are-easy-access-for-managers-and-hackers/.

[18] *See e.g.* John Leyden, *Half Baked Security: Hackers Can Hijack Your Smart Aga Oven 'With a Text Message,'* THE REGISTER (April 13, 2017), https://www.theregister.co.uk/2017/04/13/aga_oven_iot_insecurity/.

including unfair and deceptive privacy and security practices.[19] In the context of IoT security, this means that companies should maintain a reasonable security program and keep the promises they make to consumers concerning the security of their devices. The FTC also enforces sector-specific statutes that protect certain health, credit, financial, and children's information, and has issued regulations implementing each of these statutes.[20]

The FTC has used its authority under these laws to protect consumers from insecure IoT devices.[21] For example, in the *TRENDnet* case, the FTC alleged that the company engaged in unfair and deceptive security practices related to its Internet-connected cameras.[22] The complaint alleged that the company's failure to reasonably test and review the camera's software for security problems; failure to encrypt data in storage and transit; and failure to monitor third-party security vulnerability reports led to a breach of private video feeds.[23] Likewise, in the *ASUS* case, the FTC alleged that the company's failure to reasonably secure its routers led to the unauthorized access of consumers' home networks.[24] The FTC's enforcement actions send an important message to companies about the need to secure and protect Internet-connected devices.

The FTC also has pursued numerous policy initiatives designed to enhance device security in an Internet-connected world. For example, the FTC has hosted workshops on the Internet of Things generally,[25] mobile security,[26] drones,[27] connected TVs,[28] ransomware,[29] and

---

[19] 15 U.S.C. § 45. (For an unfair act or practice to violate Section 5 of the FTC Act it must "cause[] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." Additionally, deception requires a material representation, omission, or practice that is likely to mislead consumers, who are acting reasonably under the circumstances. *See* Fed. Trade Comm'n, *Policy Statement on Deception* (Oct. 14, 1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.)

[20] *See, e.g.*, Health Breach Notification Rule, 16 C.F.R. Part 318 *et seq.* (health information breach notification); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*. and 16 C.F.R. Part 600 (consumer reporting information security and privacy); Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. Part 314 *et seq*. (financial information security); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq*. and 16 C.F.R. Part 312 (children's online information security and privacy).

[21] *See e.g.*, VTech Electronics Ltd., FTC No. 1623032 (Jan 8, 2018) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/162-3032/vtech-electronics-limited; TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter; ASUSTeK Computer, Inc., FTC No. 1423156 (Feb. 26, 2016) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter; and VIZIO, Inc., No. 2:17-cv-00758 (Feb. 6, 2017) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc.

[22] TRENDnet, Inc., *supra n. 22.*

[23] *Id*.

[24] ASUSTeK Computer, Inc., *supra n.* 22.

[25] *See generally*, FTC IOT REPORT; *see also* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Nov. 19, 2013) (workshop), https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[26] MOBILE SECURITY REPORT at 18.

[27] FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: DRONES (Oct. 13, 2016) (workshop), https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones.

[28] FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: SMART TV (Dec. 7, 2016) (workshop), https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv.

[29] FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: RANSOMWARE (Sept. 7, 2016) (workshop), https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware.

connected cars.[30] In its staff report from 2015 on the Internet of Things, the FTC made several recommendations for security best practices, including recommendations that companies conduct risk assessments, test their security measures before launching their products, train employees on security, and monitor products throughout their life cycle.[31] In a more recent report on mobile device updates, the FTC discussed the complex and often time-consuming process that companies face when updating mobile devices.[32] While noting that industry participants have taken steps to streamline the process, the report recommends that manufacturers consider taking additional steps to deliver security updates to user devices faster. It also recommends that manufacturers consider telling users how long a device will receive security updates and when update support is ending.[33]

To encourage consumers to implement security updates, last year the FTC held its *IoT Home Inspector Challenge*, a public competition aimed at spurring the development of security update-related IoT tools.[34] The winning contestant developed a tool to enable users with limited technical expertise to scan their home Wi-Fi and Bluetooth networks to identify and inventory connected devices. The tool would also flag devices with out-of-date software and other common vulnerabilities, and provide instructions to consumers on how to update each of their devices and fix other vulnerabilities.[35]

Finally, the FTC engages in consumer and business education regarding IoT device security. On the business education front, the Commission launched its *Start with Security* initiative,[36] *Stick with Security* blog series,[37] and "*Careful Connections*" IoT guidance,[38] which apply to businesses considering security issues in the IoT space. For example, the Commission's *Careful Connections* guide emphasizes a risk-based approach to device security, encouraging device manufacturers to evaluate the risks to their devices and prioritize the allocation of security

---

[30] FED. TRADE COMM'N, CONNECTED CARS: PRIVACY, SECURITY ISSUES RELATED TO CONNECTED, AUTOMATED VEHICLES (Jun. 28, 2017) (workshop), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.

[31] *See generally*, FTC IOT REPORT.

[32] *See generally*, MOBILE SECURITY REPORT.

[33] *Id.* at 71-72.

[34] *See* FTC Notice of IoT Home Inspector Challenge, 82 Fed. Reg. 840-2, 840-41 (Jan. 4, 2017), https://www.ftc.gov/system/files/documents/feeral_register_noticies/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

[35] *FTC Announces Winner of its Internet of Things Home Device Security Contest*, Fed. Trade Comm'n (July 26, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

[36] FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015) [hereinafter START WITH SECURITY], https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf.

[37] Thomas B. Pahl, *Stick With Security*, FTC BUSINESS BLOG (Sept. 22, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/09/stick-security-put-procedures-place-keep-your-security.

[38] FED. TRADE COMM'N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (Jan. 2015) [hereinafter CAREFUL CONNECTIONS], https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

resources where they are most needed.[39] On the consumer education front, a consumer education blog post describes the 2016 Mirai malware attack, in which the Mirai botnet, as described above, attacked a service used by a number of popular websites like Netflix, PayPal, and Twitter, knocking them offline. The education piece urged consumers to change default settings and passwords and download the latest security updates for their IoT devices.[40]

III. Discussion

The CPSC requests comment on numerous issues. This comment focuses in particular on three: (1) What are some best practices for predicting and mitigating against safety hazards? (2) How can the CPSC encourage consumers to register for safety alerts and recall information? (3) What is the appropriate role of government in IoT security?

A. What are best practices for predicting and mitigating against safety hazards?

The FTC has provided IoT manufacturers with a host of guidance on how to predict and mitigate against privacy, security, and safety hazards. The discussion in this section is premised on the notion that there is no "one size fits all" approach to securing IoT devices. The level of reasonable security will depend on many factors, including the magnitude of potential risks, the likelihood of such risks, and the availability of low-cost tools to address the risks. This comment focuses on guidance in three areas in particular: risk assessment; reasonable vendor oversight for devices and other interdependent products; and software updates, product "expiration" dates, and default settings.

1. Risk Assessment

As the CPSC is well aware, a risk assessment is a starting point for a company to evaluate its security program. A risk assessment can help identify reasonably foreseeable threats and hazards, and solutions for mitigating against such threats and hazards. While the IoT industry is relatively new, companies have been conducting assessments to identity and mitigate against threats and hazards for several years. Companies can build on 20 years of lessons learned by security experts, who have already identified low-cost solutions to some common concerns raised by the Internet of Things.[41]

One example of a reasonably foreseeable risk is that hackers can compromise user credentials to take over an IoT device.[42] The FTC has recommended that companies test

---

[39] CAREFUL CONNECTIONS at 1-2.
[40] Ari Lazarus, *What You Need to Know to Secure Your IoT Devices*, FTC CONSUMER BLOG (Dec. 7, 2016), https://www.consumer.ftc.gov/blog/2016/12/what-you-need-know-secure-your-iot-devices.
[41] *See* CAREFUL CONNECTIONS at 2 (*E.g.* apply standard encryption techniques, apply "salt" to hashed data, and consider rate limiting).
[42] *See* FTC cases concerning the security of credentials, such as Twitter, Inc., FTC No. 0923093 (Mar. 11, 2011) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation; Reed Elsevier, Inc., FTC No. 052094 (Aug. 1, 2008), https://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter; Guidance Software, Inc., FTC No. 0623057 (April 3, 2007), https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation; and Twitter, Inc., FTC No.

authentication techniques and consider whether techniques, such as multi-factor authentication (such as a password and a code sent to a phone) or biometric authentication, are appropriate.[43] The FTC has also recommended that companies consider risks at the point where a service communicates with an IoT device, such as the interface between the device and the cloud.[44] Security experts have long warned against attack vectors such as cross-site scripting attacks, where malicious scripts are injected into otherwise trusted websites, and cross-site request forgery attacks, where unauthorized commands are sent from a user the website trusts.[45]

Finally, the FTC has recommended that companies test a product's security measures before launch. There are readily available, free or cost-effective tools for most basic security testing tasks—network scanning for open ports, reverse engineering of programming code, checking password strength, and vulnerability scans.[46]

2. Service Provider Oversight

While security protections are generally the responsibility of the manufacturer, IoT devices often are a product of components and software from a variety of service providers.[47] Prior to selling their products to consumers, IoT manufacturers should take reasonable measures to evaluate the overall security of those products, including any risks that their service providers might introduce.[48] Companies should provide oversight by exercising due diligence in their selection of service providers, incorporating security standards into their contracts, and taking reasonable steps to verify compliance with those security standards on an ongoing basis.[49]

In circumstances where companies have failed reasonably to oversee the security practices of their service providers, the FTC has taken action.[50] For example, in its case against *BLU Products*, the FTC alleged that a mobile device manufacturer had violated Section 5 of the FTC Act by failing to maintain reasonable security when, among other things, it failed to exercise oversight of its service provider.[51] In part, the FTC alleged that the company did not even put in place basic contractual provisions requiring its service providers to maintain

---

0923093 (Mar. 11, 2011) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation.

[43] CAREFUL CONNECTIONS at 3.

[44] *Id.* at 4.

[45] *Id.* Fuzzing – a testing method that sends a device or system unexpected input data to detect possible defects – is one example of an approach recommended by security experts to addressing these issues as well as discovering other implementation bugs. *See also*, *Fuzzing*, Open Web Application Security Project, https://www.owasp.org/index.php/Fuzzing.

[46] *Id.* at 5.

[47] *Se,e e.g.*, CPSC EMERGING TECHNOLOGIES REPORT at 6.

[48] CAREFUL CONNECTIONS at 1 ("There's no one-size-fits all checklist to guarantee the security of connected devices. What's reasonable will depend on a number of variables, including the kind and amount of information that's collected, the type of functionality involved, and the potential security risks.").

[49] START WITH SECURITY at 11.

[50] BLU Products, FTC No. 1723025 (April 30, 2018) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/172-3025/blu-products-samuel-ohev-zion-matter; Lenovo, Inc., FTC No. 1523134 (Sept. 13, 2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3134/lenovo-inc; and Upromise, Inc., FTC No. 1023116 (April 3, 2012), https://www.ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc.

[51] BLU Products, *supra* n. 50.

reasonable security. As a result of the company's alleged failures, consumer data was put at an unreasonable risk of unauthorized access. In this case consumers' text message contents, call and text logs, and real-time location were shared with a Chinese service provider that did not have a business need for the information, in violation of the company's privacy policy.[52]

As another example, in the FTC's recent case against *Lenovo*, the Commission alleged that Lenovo preinstalled third-party ad-injecting software on its laptops that created serious security vulnerabilities.[53] The complaint noted that, even after its service provider informed Lenovo of security problems during the development of the software, Lenovo did not seek further information and approved the software's use on Lenovo laptops.[54] This was one factor, among others, cited in the complaint alleging that Lenovo violated Section 5 by failing to implement reasonable security in overseeing its vendors.[55]

3. Ongoing Oversight, Updating, and Patching

The FTC has recommended that companies have an ongoing process to keep up with security practices as threats, safety hazards, technologies, and business models evolve. This involves at least two components.

First, companies should take steps to stay abreast of threats identified in the marketplace by, for example, signing up for email updates from trusted sources; checking free databases of vulnerabilities identified by security researchers; and maintaining a channel through which security researchers can reach out about risks.[56] Indeed, in many cases, the FTC has alleged, among other things, that the failure to maintain an adequate process for receiving and addressing security vulnerability reports from security researchers and academics is an unreasonable practice, in violation of Section 5 of the FTC Act.[57]

Second, companies should take reasonable steps to address threats to privacy, security and safety after launching products, including by issuing updates and patches. In our recently conducted study of mobile security updates, we found that the security update process varies significantly among mobile device manufacturers, and although they have made improvements, bottlenecks remain.[58] We encouraged all actors in the ecosystem to ensure that devices receive security updates for a period of time that is consistent with consumers' reasonable expectations. Such support should be a shared priority, reflected in policies, practices, and contracts among all parties involved in the creation of a device.[59] We also recommended that industry streamline the

---

[52] *Id.*
[53] Lenovo, Inc., *supra* n. 50.
[54] *Id.*
[55] While the BLU and Lenovo cases involve privacy and security, the same types of oversight of service providers would help prevent them from introducing safety hazards into IoT devices.
[56] CAREFUL CONNECTIONS at 7.
[57] *See e.g.* HTC America, FTC No. 1223049 (July 2, 2013) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter; and TRENDnet, Inc. FTC No. 1223090 (Feb. 7, 2014) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
[58] MOBILE SECURITY REPORT at 65.
[59] *Id.* at 69.

security update process. In particular, we noted that companies should patch vulnerabilities in security-only updates when the benefits of more immediate action outweigh the convenience of a bundling a security update with a functionality update.[60] Finally, we recommended that device manufacturers consider giving consumers more and better information about security update support.[61] Specifically, we recommended that manufacturers interested in providing security update information consider adopting and disclosing minimum guaranteed security support periods (and update frequency) for their devices.[62] We further recommended that they consider giving device owners prompt notice when security support is about to end (and when it has ended), so that consumers can make informed decisions about device replacement or post-support use.[63]

B. How can the CPSC encourage consumers to sign up for safety alert and recall information?

Although manufacturers can update some devices automatically, many devices require consumers to take affirmative steps to install the update. In particular, consumers must know how – and where – to check for security updates and how to install them. As the number of devices within the home multiply, the task of updating devices could become increasingly daunting. As noted above, in 2017, the FTC sponsored a prize competition under the America Competes Act to assist consumers and drive innovation in this area.[64] Encouraging the development of tools that allow consumers to monitor and maintain the security of their personal IoT devices will likely bring more general awareness to the issue, in addition to direct benefits to consumers that adopt those tools.

BCP staff recommends that the CPSC consider how companies might provide consumers with the opportunity to sign up for communications regarding safety notifications and recalls for IoT devices. Such a process could borrow from CPSC's existing process of allowing consumers to sign up for safety notifications regarding infant and toddler products.[65] That process in part requires manufacturers and retailers of durable infant and toddler products to provide consumers with a safety registration card for mail-in registration. The registration card must also include an URL for online registration.[66] Given that consumers purchasing IoT devices necessarily have an Internet connection, however, it is likely that online registration would be a more effective option in the IoT space.[67]

---

[60] *Id.* at 71.
[61] *Id.*
[62] *Id.*
[63] *Id.* at 71-72.
[64] *See* 82 Fed. Reg. 840 (2017).
[65] 74 Fed. Reg. 68677. *See also, Consumer Registration Cards for Durable Infant or Toddler Products*, CONSUMER PROD. SAFETY COMM'N, https://www.cpsc.gov/Business--Manufacturing/Business-Education/Durable-Infant-or-Toddler-Products/Durable-Infant-or-Toddler-Product-Consumer-Registration-Cards/.
[66] *Id.*
[67] For example, some panelists at the CPSC IOT HEARING raised the opportunities for application interfaces, pop-up notifications, and on-device alerts. CONSUMER PROD. SAFETY COMM'N, PUBLIC HEARING ON THE "INTERNET OF THINGS AND CONSUMER PRODUCT HAZARDS," (May 16, 2018) [hereinafter CPSC IOT HEARING], https://www.youtube.com/watch?v=7RdbpJ_eD98. Additionally, many online retailers have a direct

Some consumers may be dissuaded from registering on the expectation that they will receive unwanted marketing communications. Indeed, a recent survey showed that, while many consumers like receiving marketing communications, 12 percent of consumers do not register products because they do not want to share their personal information.[68] BCP staff recommends that, to address potential concerns of these consumers, the CPSC should consider how companies might offer consumers a choice, during the product registration process, about whether they want to receive marketing communications.[69]

C. What is the appropriate role of government in promoting IoT safety?

At the CPSC's IoT hearing, many panelists discussed the value of regulation and IoT-specific standards.[70] Although BCP staff does not take a position on whether or not the CPSC should implement regulations relating to IoT device hazards, to the extent the CPSC considers such regulation, we suggest that any such approach be technology-neutral and sufficiently flexible so that it does not become obsolete as technology changes.

In addition, to the extent that the CPSC considers certification requirements for IoT devices,[71] the CPSC should consider requiring manufacturers to publicly set forth the standards to which they adhere. Such disclosures would improve transparency and provide consumers with information to better evaluate the safety and security of their IoT products. The FTC could use its authority under the FTC Act to take action against companies that misrepresent their security practices in their certifications. This additional tool would provide an enforcement backstop to help ensure that companies comply with their certifications. Examples of enforceable statements to consumers could include statements on websites, on a retail packaging, on the device itself, or in the user interface of the device.

---

relationship with customers and, in some instances, might be in a better position to effectuate notice of safety recalls to purchasers.

[68] *See, e.g., New Study: Millennials and Affluent Consumers Want to Connect with Brands Immediately Post-Purchase via Mobile,* REGISTRIA (April 26, 2017) [hereinafter Registria survey], http://www.marketwired.com/press-release/new-study-millennials-affluent-consumers-want-connect-with-brands-immediately-post-purchase-2212124.htm (Registria also finds that 25 percent of survey respondents cite safety and recall notifications as the most important reason to register their product). *See also, "Should you register that new product? Product-registration cards—and the info you put on them—aren't always needed for warranty coverage,"* CONSUMER REPORTS (Dec. 2013), *available at* https://www.consumerreports.org/cro/2013/12/do-you-need-to-register-new-products-you-buy/index.htm ("When you buy a toaster or TV, or receive one as a gift, is it the manufacturer's business to ask about your income, education, hobbies, and car? Frankly, no. Nevertheless, many products include registration cards harvesting personal information that companies then sell to marketers. The companies get money; you get peppered with spam and sales pitches.").

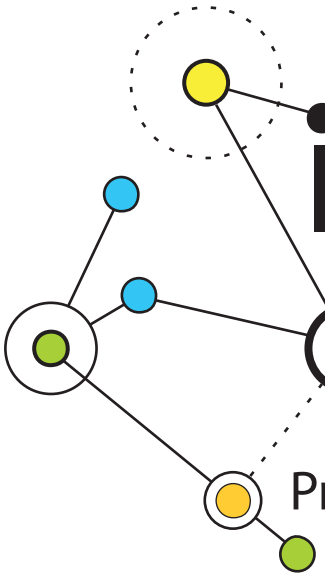
[69] 15 U.S.C. § 2056 (Consumer Product Safety Standards). *See also, Contact/FAQ,* Consumer Prod. Safety Comm'n, https://www.cpsc.gov/About-CPSC/Contact-Information (discussing the CPSC's authority to develop voluntary standards, issue mandatory standards, and research potential hazards), and *Voluntary Standards,* Consumer Prod. Safety Comm'n, https://www.cpsc.gov/Regulations-Laws--Standards/Voluntary-Standards/ (discussing the development of voluntary standards in collaboration with stakeholders, such as industry groups, government agencies, and consumer groups).

[70] CPSC IOT HEARING, https://www.youtube.com/watch?v=7RdbpJ_eD98.

[71] 83 Fed. Reg. 13122 (Mar. 27, 2018) ("Should certification to appropriate standards be required before IoT devices are allowed in the marketplace?").

IV. Conclusion

BCP staff hopes that this information has been of assistance in furthering CPSC's inquiry into protecting consumers from the hazards associated with Internet-connected devices. The FTC continues to devote substantial resources in this area and looks forward to working with CPSC and other stakeholders to foster competition and innovation in the IoT marketplace while protecting the safety of consumers.

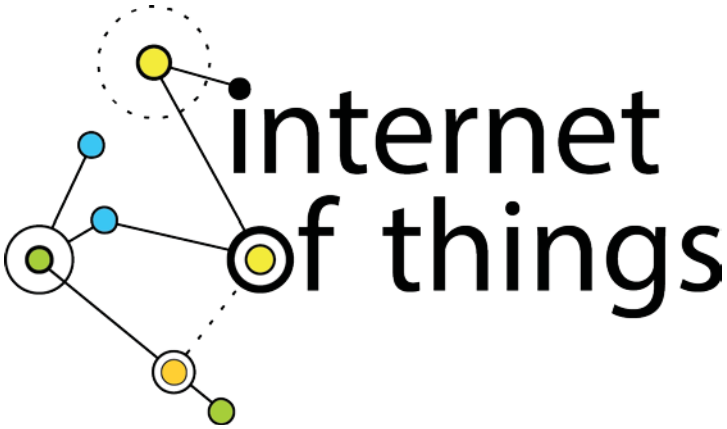


internet of things

Privacy & Security in a Connected World

FTC Staff Report

JANUARY 2015



FTC Staff Report
January 2015

Table of Contents

Executive Summary

The Internet of Things ("IoT") refers to the ability of everyday objects to connect to the Internet and to send and receive data. It includes, for example, Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day.

Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.

Given these developments, the FTC hosted a workshop on November 19, 2013 – titled *The Internet of Things: Privacy and Security in a Connected World*. This report summarizes the workshop and provides staff's recommendations in this area.[1] Consistent with the FTC's mission to protect consumers in the commercial sphere and the focus of the workshop, our discussion is limited to IoT devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, nor does it address broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Workshop participants discussed benefits and risks associated with the IoT. As to benefits, they provided numerous examples, many of which are already in use. In the health arena, connected medical devices can allow consumers with serious medical conditions to work

[1] Commissioner Wright dissents from the issuance of this Staff Report. His concerns are explained in his separate dissenting statement.

with their physicians to manage their diseases. In the home, smart meters can enable energy providers to analyze consumer energy use, identify issues with home appliances, and enable consumers to be more energy-conscious. On the road, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership. Participants generally agreed that the IoT will offer numerous other, and potentially revolutionary, benefits to consumers.

As to risks, participants noted that the IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety. Participants also noted that privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. In particular, some panelists noted that companies might use this data to make credit, insurance, and employment decisions. Others noted that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption.

In addition, workshop participants debated how the long-standing Fair Information Practice Principles ("FIPPs"), which include such principles as notice, choice, access, accuracy, data minimization, security, and accountability, should apply to the IoT space. The main discussions at the workshop focused on four FIPPs in particular: security, data minimization, notice, and choice. Participants also discussed how use-based approaches could help protect consumer privacy.

1. Security

There appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected and the costs of remedying the security vulnerabilities. Commission staff encourages companies to consider adopting the best practices highlighted by workshop participants, including those described below.

First, companies should build security into their devices at the outset, rather than as an afterthought. As part of the security by design process, companies should consider: (1) conducting a privacy or security risk assessment; (2) minimizing the data they collect and retain; and (3) testing their security measures before launching their products. Second, with respect to personnel practices, companies should train all employees about good security, and ensure that security issues are addressed at the appropriate level of responsibility within the organization. Third, companies should retain service providers that are capable of maintaining reasonable security and provide reasonable oversight for these service providers. Fourth, when companies identify significant risks within their systems, they should implement a defense-in-depth approach, in which they consider implementing security measures at several levels. Fifth, companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network. Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

2. Data Minimization

Data minimization refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it. Although some participants expressed concern that requiring data minimization could curtail innovative uses of data, staff agrees with the participants who stated that companies should consider reasonably limiting their collection and retention of consumer data.

Data minimization can help guard against two privacy-related risks. First, larger data stores present a more attractive target for data thieves, both outside and inside a company – and increases the potential harm to consumers from such an event. Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations.

To minimize these risks, companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data. However, recognizing the need to balance future, beneficial uses of data with privacy protection, staff's recommendation on data minimization is a flexible one that gives companies many options. They can decide not to collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options will fulfill its business goals, it can seek consumers' consent for collecting additional, unexpected categories of data, as explained below.

3. Notice and Choice

The Commission staff believes that consumer choice continues to play an important role in the IoT. Some participants suggested that offering notice and choice is challenging in the IoT because of the ubiquity of data collection and the practical obstacles to providing information without a user interface. However, staff believes that providing notice and choice remains important.

This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits. This principle applies equally to the Internet of Things.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface and recognizes that there is no one-size-fits-all approach. Some options include developing video tutorials, affixing QR codes on devices, and providing choices at point of sale, within set-up wizards, or in a privacy dashboard. Whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents. In addition, companies may want to consider using a combination of approaches.

Some participants expressed concern that even if companies provide consumers with choices only in those instances where the collection or use is inconsistent with context, such an

approach could restrict unexpected new uses of data with potential societal benefits. These participants urged that use limitations be considered as a supplement to, or in lieu of, notice and choice. With a use-based approach, legislators, regulators, self-regulatory bodies, or individual companies would set "permissible" and "impermissible" uses of certain consumer data.

Recognizing concerns that a notice and choice approach could restrict beneficial new uses of data, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. In addition, if a company collects a consumer's data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. Furthermore, the Commission protects privacy through a use-based approach, in some instances. For example, it enforces the Fair Credit Reporting Act, which restricts the permissible uses of consumer credit report information under certain circumstances. The Commission also applies its unfairness authority to challenge certain harmful uses of consumer data.

Staff has concerns, however, about adopting a pure use-based model for the Internet of Things. First, because use-based limitations are not comprehensively articulated in legislation, rules, or widely-adopted codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful. Second, use limitations alone do not address the privacy and security

risks created by expansive data collection and retention. Finally, a pure use-based model would not take into account consumer concerns about the collection of sensitive information.[2]

The establishment of legislative or widely-accepted multistakeholder frameworks could potentially address some of these concerns. For example, a framework could set forth permitted or prohibited uses. In the absence of consensus on such frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

4. Legislation

Participants also discussed whether legislation over the IoT is appropriate, with some participants supporting legislation, and others opposing it. Commission staff agrees with those commenters who stated that there is great potential for innovation in this area, and that IoT-specific legislation at this stage would be premature. Staff also agrees that development of self-regulatory programs designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, in light of the ongoing threats to data security and the risk that emerging IoT technologies might amplify these threats, staff reiterates the Commission's previous recommendation for Congress to enact strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools and to provide notification to consumers when there is a security breach. General data security legislation should protect against unauthorized access to both personal information and device functionality itself. For

[2] In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards, which the Commission previously recommended in its 2012 privacy report. Although the Commission currently has authority to take action against some IoT-related practices, it cannot mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness. Commission staff thus again recommends that Congress enact broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as how to provide choices to consumers about data collection and use practices.[3]

In the meantime, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
  The Commission enforces the FTC Act, the FCRA, the health breach notification provisions of the HI-TECH Act, the Children's Online Privacy Protection Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws.

- **Consumer and business education:**
  The Commission staff will develop new consumer and business education materials in this area.

[3] Commissioner Ohlhausen does not agree with the recommendation for baseline privacy legislation. *See infra* note 191.

- **Participation in multi-stakeholder groups:**
  Currently, Commission staff is participating in multi-stakeholder groups that are considering guidelines related to the Internet of Things, including on facial recognition and smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers.

- **Advocacy:**
  Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area.

Background

Technology is quickly changing the way we interact with the world around us. Today, companies are developing products for the consumer market that would have been unimaginable a decade ago: Internet-connected cameras that allow you to post pictures online with a single click; home automation systems that turn on your front porch light when you leave work; and bracelets that share with your friends how far you have biked or run during the day. These are all examples of the Internet of Things ("IoT"), an interconnected environment where all manner of objects have a digital presence and the ability to communicate with other objects and people. The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn't a mobile phone, tablet, or traditional computer.

Six years ago, for the first time, the number of "things" connected to the Internet surpassed the number of people.[1] Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.[2] Some estimate that by 2020, 90% of consumer cars will have an Internet connection, up from less than 10 percent in 2013.[3] Three and one-half billion sensors already are in the

[1] DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), *available at* http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf. These estimates include all types of connected devices, not just those aimed at the consumer market.

[2] *Id*.

[3] TELEFONICA, CONNECTED CAR INDUSTRY REPORT 2013 9 (2013), *available at* http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.

marketplace,[4] and some experts expect that number to increase to trillions within the next decade.[5] All of these connected machines mean much more data will be generated: globally, by 2018, mobile data traffic will exceed fifteen exabytes – about 15 quintillion bytes – each month.[6] By comparison, according to one estimate, an exabyte of storage could contain 50,000 years' worth of DVD-quality video.[7]

These new developments are expected to bring enormous benefits to consumers. Connected health devices will allow consumers with serious health conditions to work with their physicians to manage their diseases. Home automation systems will enable consumers to turn off the burglar alarm, play music, and warm up dinner right before they get home from work. Connected cars will notify first responders in the event of an accident. And the Internet of Things may bring benefits that we cannot predict.

However, these connected devices also will collect, transmit, store, and potentially share vast amounts of consumer data, some of it highly personal. Given the rise in the number and types of connected devices already or soon to be on the market, the Federal Trade Commission ("FTC" or "Commission") announced in April 2013 that it would host a workshop on the privacy and security issues associated with such devices and requested public input about the issues to

---

[4] *See* Stanford Univ., *TSensors Summit™ for Trillion Sensor Roadmap* 1 (Oct. 23-25, 2013), *available at* http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf.

[5] *Id*.

[6] CISCO, CISCO VISUAL NETWORKING INDEX: GLOBAL MOBILE DATA TRAFFIC FORECAST UPDATE, 2013–2018 3 (2014), *available at* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white_paper_c11-520862.pdf.

[7] University of Bristol, Exabyte Informatics, *available at* http://www.bris.ac.uk/research/themes/exabyte-informatics.html.

consider.[8] In response to the request for comment, staff received twenty-nine public comments[9] from a variety of consumer advocacy groups, academics, and industry representatives. The workshop – titled *The Internet of Things: Privacy and Security in a Connected World* – took place on November 19, 2013, and featured panels of academics, researchers, consumer advocates, and representatives from government and industry.[10]

The workshop consisted of four panels,[11] each of which focused on a different aspect of the IoT.[12] The first panel, "The Smart Home,"[13] looked at an array of connected devices, such as home automation systems and smart appliances. The second panel, "Connected Health and Fitness,"[14] examined the growth of increasingly connected medical devices and health and fitness products, ranging from casual wearable fitness devices to connected insulin pumps. The third panel, "Connected Cars,"[15] discussed the different technologies involved with connected

---

[8] Press Release, FTC, FTC Seeks Input on Privacy and Security Implications of the Internet of Things (Apr. 17, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/04/ftc-seeks-input-privacy-and-security-implications-internet-things.

[9] Pre-workshop comments ("#484 cmt.") are available at http://www.ftc.gov/policy/public-comments/initiative-484.

[10] For a description of the workshop, *see* http://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[11] In addition to the four panels, workshop speakers included Keith Marzullo of the National Science Foundation ("Marzullo"), who gave an overview of the IoT space (Transcript of Workshop at 15-34); Carolyn Nguyen ("Nguyen") of Microsoft Corp., who discussed contextual privacy and its implications for the IoT (Transcript of Workshop at 35-51); and Vinton "Vint" Cerf ("Cerf") of Google Inc., who gave the workshop's Keynote Address (Transcript of Workshop at 118-153).

[12] A complete transcript of the proceeding is available at http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf. Videos of the workshop also are available at http://www.ftc.gov/news-events/audio-video/ftc-events.

[13] Transcript of Workshop at 52-115.

[14] *Id.* at 164-234.

[15] *Id.* at 235-291.

cars, including Event Data Recorders ("EDRs")[16] and other vehicle "telematics," a term that refers to data collection, transmission, and processing technologies for use in vehicles. Finally, the fourth panel, "Privacy and Security in a Connected World,"[17] discussed the broader privacy and security issues raised by the IoT.

Following the workshop, the Commission invited comments on the issues raised by the panels.[18] In response, staff received seventeen public comments from private citizens, trade organizations, and privacy advocates.[19]

This report summarizes the workshop and provides staff's recommendations in this area. Section II of this report discusses how we define the "Internet of Things." Section III describes some of the benefits and risks of the new technologies that are part of the IoT phenomenon. Section IV examines the application of existing privacy principles to these new technologies, and Section V addresses whether legislation would be appropriate in this area. Sections IV and V begin by discussing the views of written commenters and workshop speakers (collectively, "participants"), and then set forth staff recommendations. These recommendations focus on the types of products and services consumers are likely to encounter today and in the foreseeable future. We look forward to continuing to explore privacy issues as new IoT technologies come to market.

---

[16] An EDR is "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (*e.g.*, vehicle speed vs. time) or during a crash event . . . intended for retrieval after the crash event." 49 C.F.R. § 563.5.

[17] Transcript of Workshop at 292-364.

[18] Press Release, FTC, FTC Seeks Comment on Issues Raised at Internet of Things Workshop (Dec. 11, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/12/ftc-seeks-comment-issues-raised-internet-things-workshop.

[19] Post-workshop comments ("#510 cmt.") are available at http://www.ftc.gov/policy/public-comments/initiative-510.

What is the "Internet of Things"?

Although the term "Internet of Things" first appeared in the literature in 2005,[20] there is still no widely accepted definition.[21] One participant described the IoT as the connection of "physical objects to the Internet and to each other through small, embedded sensors and wired and wireless technologies, creating an ecosystem of ubiquitous computing."[22] Another participant described it as including "embedded intelligence" in individual items that can detect changes in their physical state.[23] Yet another participant, noting the lack of an agreed-upon definition of the IoT, observed, "[w]hat all definitions of IoT have in common is that they focus on how computers, sensors, and objects interact with one another and process data."[24]

The IoT includes consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines. For example, the term IoT can include the type of Radio Frequency Identification ("RFID") tags that businesses place on products in stores to monitor inventory; sensor networks to monitor electricity use in hotels; and Internet-connected jet engines and drills on oil rigs. Moreover, the "things" in the IoT generally do not include desktop or laptop computers and their close analogs, such as smartphones and tablets, although these devices are often employed to control or communicate with other "things."

---

[20] *See* Remarks of Marzullo, Transcript of Workshop at 19.

[21] *See Comment of ARM/AMD*, #510 cmt. #00018 at 1.

[22] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 1.

[23] Remarks of Marzullo, Transcript of Workshop at 19.

[24] *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 3.

For purposes of this report, we use the term IoT to refer to "things" such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet. Consistent with the FTC's mission to protect consumers in the commercial sphere, our discussion of IoT is limited to such devices that are sold to or used by consumers. Accordingly, the report does not discuss devices sold in a business-to-business context, such as sensors in hotel or airport networks; nor does it discuss broader machine-to-machine communications that enable businesses to track inventory, functionality, or efficiency.

Benefits & Risks

Like all technologies, the Internet of Things has benefits and risks. To develop policy approaches to this industry, one must understand both. Below is a summary of the benefits and risks of IoT, both current and potential, highlighted by workshop participants.

Benefits

Most participants agreed that the IoT will offer numerous, and potentially revolutionary, benefits to consumers.[25] One area in which these benefits appear highly promising is health care.[26] For example, insulin pumps and blood-pressure cuffs that connect to a mobile app can enable people to record, track, and monitor their own vital signs, without having to go to a doctor's office. This is especially beneficial for aging patients, for whom connected health devices can provide "treatment options that would allow them to manage their health care at home without the need for long-term hospital stays or transition to a long-term care facility."[27] Patients can also give caregivers, relatives, and doctors access to their health data through these apps, resulting in numerous benefits. As one panelist noted, connected health devices can "improve quality of life and safety by providing a richer source of data to the patient's doctor for diagnosis and treatment[,] . . . improve disease prevention, making the healthcare system more efficient and driving costs down[,] . . . [and] provide an incredible wealth of data, revolutionizing

[25] *See Comment of Future of Privacy Forum*, #484 cmt. #00013 at 4; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 2.

[26] *See Comment of AT&T Inc.*, #484 cmt. #00004 at 5.

[27] *Comment of Med. Device Privacy Consortium*, #484 cmt. #00022 at 1.

medical research and allowing the medical community to better treat, and ultimately eradicate, diseases."[28]

Recent studies demonstrate meaningful benefits from connected medical devices. One workshop participant said that "one of the most significant benefits that we have from this connected world [is] the ability to . . . draw the patients in and engage them in their own care."[29] Another participant described a clinical trial showing that, when diabetic patients used connected glucose monitors, and their physicians received that data, those physicians were five times more likely to adjust medications, resulting in better disease management and substantial financial savings for patients. He stated that the clinical trial demonstrated that diabetic patients using the connected glucose monitor reduced their average blood sugar levels by two points and that, by comparison, the Food and Drug Administration ("FDA") considers medications that reduce blood sugar by as little as one half point to be successful.[30]

Consumers can benefit from the IoT in many other ways. In the home, for example, smart meters can enable energy providers to analyze consumer energy use and identify issues with home appliances, "even alerting homeowners if their insulation seems inadequate compared to that of their neighbors,"[31] thus empowering consumers to "make better decisions about how they use electricity."[32] Home automation systems can provide consumers with a "single platform that

[28] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 16.

[29] *See* Remarks of Stan Crosley, Indiana Univ. ("Crosley"), Transcript of Workshop at 199.

[30] *See* Remarks of Anand Iyer, WellDoc Communications, Inc. ("Iyer"), Transcript of Workshop at 188–189.

[31] *Comment of AT&T Inc.*, #484 cmt. #00004 at 4-5.

[32] Remarks of Eric Lightner, Department of Energy ("Lightner"), Transcript of Workshop at 54.

can connect all of the devices within the home, [with] a single app for controlling them."[33] Connected ovens allow consumers to "set [their] temperatures remotely . . . , go from bake to broil . . . , [and] monitor [their] products from various locations inside . . . and outside [their] home[s]."[34] Sensors known as "water bugs" can notify consumers if their basements have flooded,[35] and wine connoisseurs can monitor the temperature in their wine cellars to preserve their finest vintages.[36]

On the road, connected cars will increasingly offer many safety and convenience benefits to consumers. For example, sensors on a car can notify drivers of dangerous road conditions, and software updates can occur wirelessly, obviating the need for consumers to visit the dealership.[37] Connected cars also can "offer real-time vehicle diagnostics to drivers and service facilities; Internet radio; navigation, weather, and traffic information; automatic alerts to first responders when airbags are deployed; and smartphone control of the starter and other aspects of the car."[38] In the future, cars will even drive themselves. Participants discussed the ability of self-driving cars to create safety benefits. For example, rather than having error-prone humans decide which car should go first at a four-way stop sign, self-driving cars will be able to figure out who should

[33] Remarks of Jeff Hagins, SmartThings ("Hagins"), Transcript of Workshop at 64.

[34] Remarks of Michael Beyerle, GE Appliances ("Beyerle"), Transcript of Workshop at 60.

[35] *See* Remarks of Scott Peppet, Univ. of Colorado School of Law ("Peppet"), Transcript of Workshop at 167.

[36] *See* Remarks of Cerf, Transcript of Workshop at 132.

[37] *See* Remarks of Christopher Wolf, Future of Privacy Forum ("Wolf"), Transcript of Workshop at 247-48.

[38] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 13.

go first according to a standard protocol.[39] They would also allow people with visual impairments to use their own cars as a mode of transportation.[40]

Risks

Despite these important benefits, there was broad agreement among participants that increased connectivity between devices and the Internet may create a number of security and privacy risks.[41]

SECURITY RISKS

According to panelists, IoT devices may present a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating safety risks. Although each of these risks exists with traditional computers and computer networks, they are heightened in the IoT, as explained further below.

First, on IoT devices, as with desktop or laptop computers, a lack of security could enable intruders to access and misuse personal information collected and transmitted to or from the

---

[39] *See* Remarks of Cerf, Transcript of Workshop at 127.

[40] *See id*. at 138.

[41] *See, e.g.*, Remarks of Craig Heffner, Tactical Network Solutions ("Heffner"), Transcript of Workshop at 73-77, 109-10; Remarks of Lee Tien, Electronic Frontier Foundation ("Tien"), Transcript of Workshop at 82-83; Remarks of Hagins, Transcript of Workshop at 92-93, 110; Remarks of Jay Radcliffe, InGuardians, Inc. ("Radcliffe"), Transcript of Workshop at 182-84; Remarks of Iyer, Transcript of Workshop at 223; Remarks of Tadayoshi Kohno, Univ. of Washington ("Kohno"), Transcript of Workshop at 244-47, 263-64; Remarks of David Jacobs, Electronic Privacy Information Center ("Jacobs"), Transcript of Workshop at 296; Remarks of Marc Rogers, Lookout, Inc. ("Rogers"), Transcript of Workshop at 344-45. *See also, e.g.*, HP, INTERNET OF THINGS RESEARCH STUDY 5 (2014), *available at* http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en ("HP Security Research reviewed 10 of the most popular devices in some of the most common IoT niches revealing an alarmingly high average number of vulnerabilities per device. Vulnerabilities ranged from Heartbleed to denial of service to weak passwords to cross-site scripting."); *id*. at 4 (noting that 80 percent of devices tested raised privacy concerns).

device. For example, new smart televisions enable consumers to surf the Internet, make purchases, and share photos, similar to a laptop or desktop computer. [42] Like a computer, any security vulnerabilities in these televisions could put the information stored on or transmitted through the television at risk. If smart televisions or other devices store sensitive financial account information, passwords, and other types of information, unauthorized persons could exploit vulnerabilities to facilitate identity theft or fraud.[43] Thus, as consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.[44]

Second, security vulnerabilities in a particular device may facilitate attacks on the consumer's network to which it is connected, or enable attacks on other systems.[45] For example,

---

[42] *See, e.g.*, Erica Fink & Laurie Segall, *Your TV might be watching you*, CNN MONEY (Aug. 1, 2013), *available at* http://money.cnn.com/2013/08/01/technology/security/tv-hack/index.html ("Today's high-end televisions are almost all equipped with 'smart' PC-like features, including Internet connectivity, apps, microphones and cameras.").

[43] *See* Mario Ballano Barcena *et al*., *Security Response, How safe is your quantified self?*, SYMANTEC (Version 1.1 – Aug. 11, 2014), *available at* www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/how-safe-is-your-quantified-self.pdf (noting risks relating to IoT including identity theft). According to the most recent statistics from the Bureau of Justice Statistics of the Department of Justice, an estimated 16.6 million Americans – about seven percent of Americans sixteen or older – experienced at least one incident of identity theft in 2012. Losses due to personal identity theft totaled $24.7 billion, billions of dollars more than the losses for all other property crimes *combined*. BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012 (Dec. 2013)), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf. Another study demonstrated that one in four people who received notice of a breach involving their personal information were victims of identity theft, a significantly higher figure than for individuals who did not receive a breach notice. *See* Javelin, 2013 Identity Fraud Report, *available at* https://www.javelinstrategy.com/brochure/276.

[44] *See, e.g.*, Remarks of Marzullo, Transcript of Workshop at 18-19 (discussing ubiquitous or pervasive computing); *id.* at 28-30 (discussing potential security vulnerabilities in devices ranging from pacemakers to automobiles); Remarks of Nguyen, Transcript of Workshop at 35 ("the first thing that really comes to mind are the sensors that are expected to be ubiquitously present and the potential for everything inanimate, whether it be in the home, in the car, or attached to the individual, to measure and transmit data").

[45] *See* Remarks of Heffner, Transcript at 113 ("[I]f I, as someone out on the Internet, can break into a device that is inside your network, I am now inside your network and I can access other things that you do care about . . . . There should never be a device on your network that you shouldn't care about the security of.").

a compromised IoT device could be used to launch a denial of service attack.[46] Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks.[47] Another possibility is that a connected device could be used to send malicious emails.[48]

Third, unauthorized persons might exploit security vulnerabilities to create risks to physical safety in some cases. One participant described how he was able to hack remotely into two different connected insulin pumps and change their settings so that they no longer delivered medicine.[49] Another participant discussed a set of experiments where an attacker could gain "access to the car's internal computer network without ever physically touching the car."[50] He described how he was able to hack into a car's built-in telematics unit and control the vehicle's engine and braking, although he noted that "the risk to car owners today is incredibly small," in part because "all the automotive manufacturers that I know of are proactively trying to address these things."[51] Although the risks currently may be small, they could be amplified as fully

---

[46] *See, e.g.*, Dick O'Brien, *The Internet of Things: New Threats Emerge in a Connected World*, SYMANTEC (Jan. 21, 2014), *available at* www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world (describing worm attacking IoT devices that connects them to a botnet for use in denial of service attacks).

[47] *Id.*

[48] *See* Paul Thomas, *Despite the News, Your Refrigerator is Not Yet Sending Spam*, SYMANTEC (Jan. 23, 2014), *available at* http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam (debunking reports that an Internet worm had used compromised IoT devices to send out spam, but adding, "While malware for IoT devices is still in its infancy, IoT devices are susceptible to a wide range of security concerns. So don't be surprised if, in the near future, your refrigerator actually does start sending spam.").

[49] *See* Remarks of Radcliffe, Transcript of Workshop at 182. *See also* Remarks of Tien, Transcript of Workshop at 82-83 ("And obviously one of the big differences between, say, a problem with your phone and a problem with your . . . diabetes pump or your defibrillator is that if it is insecure and it is subject to any kind of malware or attack, it is much more likely there would be very serious physical damage.").

[50] Remarks of Kohno, Transcript of Workshop at 245.

[51] *See id.* at 245-47, 266.

automated cars, and other automated physical objects, become more prevalent. Unauthorized access to Internet-connected cameras or baby monitors also raises potential physical safety concerns.[52] Likewise, unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home.

These potential risks are exacerbated by the fact that securing connected IoT devices may be more challenging than securing a home computer, for two main reasons. First, as some panelists noted, companies entering the IoT market may not have experience in dealing with security issues.[53] Second, although some IoT devices are highly sophisticated, many others may be inexpensive and essentially disposable.[54] In those cases, if a vulnerability were discovered after manufacture, it may be difficult or impossible to update the software or apply a patch.[55] And if an update is available, many consumers may never hear about it.[56] Relatedly, many

---

[52] *See* discussion of TRENDnet, *infra* notes 132-34 and accompanying text (FTC settlement alleging that hackers were able to access video streams from TRENDnet cameras). In another notorious incident, a hacker gained access to a video and audio baby monitor. *See* Chris Matyszczyk, *Hacker Shouts at Baby Through Baby Monitor*, CNET (Apr. 29, 2014), *available at* www.cnet.com/news/hacker-shouts-at-baby-through-baby-monitor/. *See also* Kashmir Hill, *'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users*, FORBES (Aug. 27, 2013), *available at* www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/ (recounting a similar incident).

[53] Remarks of Tien, Transcript of Workshop at 71; Remarks of Heffner, Transcript of Workshop at 73-75; Remarks of Hagins, Transcript of Workshop at 92-93.

[54] *See Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2.

[55] *See, e.g.*, Article 29 Data Protection Working Party, Opinion 8/2014 on Recent Developments on the Internet of Things 9 (Sept. 16, 2014) ("Article 29 Working Group Opinion"), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf ("For example, most of the sensors currently present on the market are not capable of establishing an encrypted link for communications since the computing requirements will have an impact on a device limited by low-powered batteries.").

[56] *Id. See also* Hill, *supra* note 52 (noting that some 40,000 of 46,000 purchasers of connected cameras had not installed a firmware update addressing a security vulnerability).

companies – particularly those developing low-end devices – may lack economic incentives to provide ongoing support or software security updates at all, leaving consumers with unsupported or vulnerable devices shortly after purchase.[57]

PRIVACY RISKS

In addition to risks to security, participants identified privacy risks flowing from the Internet of Things. Some of these risks involve the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information – risks already presented by traditional Internet and mobile commerce. Others arise from the collection of personal information, habits, locations, and physical conditions over time,[58] which may allow an entity that has not directly collected sensitive information to infer it.

The sheer volume of data that even a small number of devices can generate is stunning: one participant indicated that fewer than 10,000 households using the company's IoT home-automation product can "generate 150 million discrete data points a day"[59] or approximately one data point every six seconds for each household.[60]

---

[57] *See, e.g., Bruce Schneier, The Internet of Things Is Wildly Insecure — And Often Unpatchable,* WIRED (Jan. 6, 2014), *available at* http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem ("The problem with this process is that no one entity has any incentive, expertise, or even ability to patch the software once it's shipped. The chip manufacturer is busy shipping the next version of the chip, and the [original device manufacturer] is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn't a priority.").

[58] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 67; *Comment of Ctr. for Democracy & Tech.*, #484 cmt. #00028 at 4-5.

[59] Remarks of Hagins, Transcript of Workshop at 89.

[60] *Cf. infra* note 73 and accompanying text (discussing inferences possible from smart meter readings taken every two seconds).

Such a massive volume of granular data allows those with access to the data to perform analyses that would not be possible with less rich data sets.[61] According to a participant, "researchers are beginning to show that existing smartphone sensors can be used to infer a user's mood; stress levels; personality type; bipolar disorder; demographics (*e.g.*, gender, marital status, job status, age); smoking habits; overall well-being; progression of Parkinson's disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement."[62] This participant noted that such inferences could be used to provide beneficial services to consumers, but also could be misused. Relatedly, another participant referred to the IoT as enabling the collection of "sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals."[63] Some panelists cited to general privacy risks associated with these granular information-collection practices, including the concern that the trend towards abundant collection of data creates a "non-targeted dragnet collection from devices in the environment."[64]

Others noted that companies might use this data to make credit, insurance, and employment decisions.[65] For example, customers of some insurance companies currently may opt into programs that enable the insurer to collect data on aspects of their driving habits – such

---

[61] *See* Article 29 Working Group Opinion, *supra* note 55, at 8 ("Full development of IoT capabilities may put a strain on the current possibilities of anonymous use of services and generally limit the possibility of remaining unnoticed.").

[62] Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security & Consent*, 93 TEX. L. REV. 85, 115-16 (2014) (citations omitted) ("*Regulating the Internet of Things*"), *available at* http://www.texaslrev.com/wp-content/uploads/Peppet-93-1.pdf. Although we do not include smartphones in our definition of IoT (*see supra* p. 6), many IoT devices contain sensors similar to the sensors in smartphones, and therefore, similar types of inferences may be possible using data from IoT devices.

[63] *Comment of Elec. Privacy Info. Ctr.*, #484 cmt. #00011 at 3.

[64] Remarks of Tien, Transcript of Workshop at 67.

[65] *See* Remarks of Peppet, Transcript of Workshop at 169.

as in one case, the number of "hard brakes," the number of miles driven, and the amount of time spent driving between midnight and 4 a.m. – to help set the insurance rate.[66] Use of data for credit, insurance, and employment decisions could bring benefits – *e.g.*, enabling safer drivers to reduce their rates for car insurance or expanding consumers' access to credit – but such uses could be problematic if they occurred without consumers' knowledge or consent, or without ensuring accuracy of the data.

As a further example, one researcher has hypothesized that although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment (*e.g.*, a conscientious exerciser is a good credit risk or will make a good employee).[67] According to one commenter, it would be of particular concern if this type of decision-making were to systematically bias companies against certain groups that do not or cannot engage in the favorable conduct as much as others or lead to discriminatory practices against protected classes.[68]

Participants noted that the Fair Credit Reporting Act ("FCRA")[69] imposes certain limits on the use of consumer data to make determinations about credit, insurance, or employment, or for similar purposes.[70] The FCRA imposes an array of obligations on entities that qualify as

---

[66] *See* Peppet, *Regulating the Internet of Things*, *supra* note 62, at 106-07. *See also*, *e.g.*, Progressive, Snapshot Common Questions, *available at* http://www.progressive.com/auto/snapshot-common-questions/; StateFarm, Drive Safe & Save with In-Drive, *available at* https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/indrive.

[67] *See* Remarks of Peppet, Transcript of Workshop at 167-169.

[68] *See id.* at 93, 123-24.

[69] 15 U.S.C. § 1681 *et seq*.

[70] *See*, *e.g.*, Remarks of Crosley, Transcript of Workshop at 213; Remarks of Peppet, Transcript of Workshop at 213; Peppet, *Regulating the Internet of Things*, *supra* note 62, at 126-127.

consumer reporting agencies, such as employing reasonable procedures to ensure maximum possible accuracy of data and giving consumers access to their information.[71] However, the FCRA excludes most "first parties" that collect consumer information; thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers' connected devices and use the data to make in-house credit, insurance, or other eligibility decisions – something that could become increasingly common as the IoT develops. For example, an insurance company may offer consumers the option to submit data from a wearable fitness tracker, in exchange for the prospect of lowering their health insurance premium. The FCRA's provisions, such as those requiring the ability to access the information and correct errors, may not apply in such circumstances.

Yet another privacy risk is that a manufacturer or an intruder could "eavesdrop" remotely, intruding into an otherwise private space. Companies are already examining how IoT data can provide a window into the previously private home.[72] Indeed, by intercepting and analyzing unencrypted data transmitted from a smart meter device, researchers in Germany were

---

[71] *See* 15 U.S.C. §§1681e, 1681j.

[72] *See, e.g.*, Louise Downing, *WPP Unit, Onzo Study Harvesting Smart-Meter Data*, BLOOMBERG (May 12, 2014), *available at* http://origin-www.bloomberg.com/apps/news?pid=conewsstory&tkr=WPP:LN&sid=aPY7EUU9oD6g (reporting that the "world's biggest advertising agency" and a software company are collaborating to explore uses of smart meter data and quoting a CEO who noted, "Consumers are leaving a digital footprint that opens the door to their online habits and to their shopping habits and their location, and the last thing that is understood is the home, because at the moment, when you shut the door, that is it."). *See also Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 2-3 ("to the extent that a powerful commercial entity controls an IoT networking platform within a home or business, that positions them to collect, analyze, and act upon copious amounts of data from within traditionally private spaces.").

able to determine what television show an individual was watching.[73] Security vulnerabilities in camera-equipped devices have also raised the specter of spying in the home.[74]

Finally, some participants pointed out that perceived risks to privacy and security, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential and may result in less widespread adoption.[75] As one participant stated, "promoting privacy and data protection principles remains paramount to ensure societal acceptance of IoT services."[76]

[73] *See* Dario Carluccio & Stephan Brinkhaus, Presentation: "Smart Hacking for Privacy," 28th Chaos Communication Congress, Berlin, December 2011, *available at* https://www.youtube.com/watch?v=YYe4SwQn2GE&feature=youtu.be. Moreover, "the two-second reporting interval provides so much data that [the researchers] were able to accurately chart power usage spikes and lulls indicative of times a homeowner would be home, asleep or away." *Id.* (In most smart meter implementations, data is reported at much longer intervals, usually fifteen minutes.) In addition to the privacy concerns, as noted above, the researchers discovered that the encryption was not implemented properly and that they could alter the energy consumption data reported by the meter. *Id.*

[74] *See, e.g.*, Fink & Segall, *supra* note 42 (describing a security vulnerability in Samsung smart TVs, since patched, that "enabled hackers to remotely turn on the TVs' built-in cameras without leaving any trace of it on the screen").

[75] *See, e.g.*, *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 17-18; *Comment of CTIA – The Wireless Ass'n*, #510 cmt. #00014 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5.

[76] *Comment of GS1 US*, #484 cmt. #00030 at 4.

Application of Traditional Privacy Principles

Summary of Workshop Discussions

Participants debated how the long-standing Fair Information Practice Principles ("FIPPs") of notice, choice, access, accuracy, data minimization, security, and accountability should apply to the IoT space. While some participants continued to support the application of all of the FIPPs,[77] others argued that data minimization, notice, and choice are less suitable for protecting consumer privacy in the IoT.[78]

The FIPPs were first articulated in 1973 in a report by what was then the U.S. Department of Health, Education and Welfare.[79] Subsequently, in 1980, the Organization for Economic Cooperation and Development ("OECD") adopted a set of privacy guidelines, which embodied the FIPPs.[80] Over time, the FIPPs have formed the basis for a variety of both government and private sector initiatives on privacy. For example, both the European Union

[77] *See, e.g.*, Remarks of Michelle Chibba, Office of the Information and Privacy Commissioner, Ontario, Canada ("Chibba"), Transcript of Workshop at 329; Remarks of Jacobs, Transcript of Workshop at 328-329; *Comment of AAA*, #510 cmt. #00012 at 2; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3.

[78] *See, e.g.*, *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3.

[79] *See* FTC, PRIVACY ONLINE: A REPORT TO CONGRESS 48 n.27 (1998), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[80] *See* OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. (In 2013, the OECD updated its guidelines to address risk management, interoperability, and other issues. The update is available at http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf). *See also* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS 3-4, 43 n.25 (2000).

Directive on the protection of personal data[81] and the Health Insurance Portability and Accountability Act ("HIPAA")[82] are based, in large part, on the FIPPs. In addition, many self-regulatory guidelines include the principles of notice, choice, access, and security.[83] The Obama Administration's Consumer Privacy Bill of Rights also includes these principles,[84] as does the privacy framework set forth in the Commission's 2012 Privacy Report.[85]

Workshop discussion focused on four FIPPs in particular – data security, data minimization, notice, and choice. As to data security, there was widespread agreement on the need for companies manufacturing IoT devices to incorporate reasonable security into these devices. As one participant stated, "Inadequate security presents the greatest risk of actual consumer harm in the Internet of Things."[86] Accordingly, as another participant noted,

---

[81] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[82] Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

[83] *See, e.g.*, NETWORK ADVER. INITIATIVE, NAI CODE OF CONDUCT 2013, *available at* http://www.networkadvertising.org/2013_Principles.pdf; INTERNET ADVER. BUREAU, INTERACTIVE ADVERTISING PRIVACY PRINCIPLES (Feb. 24, 2008), *available at* http://www.iab.net/guidelines/508676/1464.

[84] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[85] FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS vii-viii (2012) ("Privacy Report"), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf. Commissioners Ohlhausen and Wright were not members of the Commission at that time and thus did not offer any opinion on that matter.

[86] *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 9 (and listing types of security measures that are already being implemented to secure the IoT).

"[s]ecurity must be built into devices and networks to prevent harm and build consumer trust in the IoT." [87]

Participants were more divided about the continuing applicability of the principles of data minimization, notice, and choice to the IoT.[88] With respect to data minimization – which refers to the concept that companies should limit the data they collect and retain, and dispose of it once they no longer need it – one participant expressed concerns that requiring fledgling companies to predict what data they should minimize would "chok[e] off potential benefits and innovation."[89] A second participant cautioned that "[r]estricting data collection with rules like data minimization could severely limit the potential opportunities of the Internet of Things" based on beneficial uses that could be found for previously-collected data that were not contemplated at the time of collection.[90] Still another participant noted that "[d]ata-driven innovation, in many ways, challenges many interpretations of data minimization where data purpose specification and use limitation are overly rigid or prescriptive."[91]

With respect to notice and choice, some participants expressed concern about its feasibility, given the ubiquity of IoT devices and the persistent and pervasive nature of the

---

[87] *Comment of Infineon Tech. N. Am. Corp.*, #510 cmt. #00009 at 2; *see also* Remarks of Rogers, Transcript of Workshop at 312 ("There are some pretty good examples out there of what happens to companies when security becomes an afterthought and the cost that companies can incur in trying to fight the damage, the cost to brand reputation, the loss of customer confidence. And there are also some great examples of companies, even in the Internet of Things, as new as it is, companies that have gotten it right and they've done well. And they've gone on to push out products where there have been no issues.").

[88] *See, e.g.*, *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. # 00021 at 2; *Comment of Info. Tech. Indus. Council*, #510 cmt. #00008 at 3-4.

[89] Remarks of Dan Caprio, McKenna, Long & Aldridge, LLP ("Caprio"), Transcript of Workshop at 339.

[90] *Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 3.

[91] *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 6–7; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013 at 5 (purpose specification and data minimization as applied to the IoT "risks unduly limiting the development of new services and the discoveries that may follow from valuable research").

information collection that they make possible. As one participant observed, when "a bunch of different sensors on a bunch of different devices, on your home, your car, your body . . . are measuring all sorts of things," it would be burdensome both for the company to provide notice and choice, and for the consumer to exercise such choice every time information was reported.[92] Another participant talked about the risk that, if patients have "to consent to everything" for a health monitoring app, "patients will throw the bloody thing away."[93] Yet another participant noted that any requirement to obtain consent could be "a barrier to socially beneficial uses of information."[94]

A related concern is that many IoT devices – such as home appliances or medical devices – have no screen or other interface to communicate with the consumer, thereby making notice on the device itself difficult, if not impossible.[95] For those devices that do have screens, the screens may be smaller than even the screens on mobile devices, where providing notice is already a challenge.[96] Finally, even if a device has screens, IoT sensors may collect data at times when the consumer may not be able to read a notice (for example, while driving).[97]

---

[92] Remarks of Peppet, Transcript of Workshop at 215–16.

[93] Remarks of Iyer, Transcript of Workshop at 230.

[94] *Comment of Software & Info. Indus. Ass'n*, #484 cmt. #00025 at 8.

[95] *See, e.g., Comment of Ctr. for Data Innovation*, #510 cmt. #00002 at 2; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 2 and 6; *Comment of Transatl. Computing Continuum Policy Alliance*, #510 cmt. #00017 at 2.

[96] *See* FTC STAFF REPORT, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 10–11 (2013) ("Mobile Disclosures Report"), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf.

[97] In addition, some participants also suggested that notice and choice is not workable for IoT products and services that are not consumer-facing – *e.g.*, a sensor network to monitor electricity use in hotels. *See, e.g.*, *Comment of GS1 US*, #484 cmt. #00030 at 5 (noting that "[i]t is difficult to anticipate how the existing mechanisms of notice and choice, both being sound principles for privacy protection, would apply to sensors. . . . [H]ow would one provide adequate notice for every embedded sensor network? How would consent be obtained?"); *Comment of Future of*

Despite these challenges, participants discussed how companies can provide data minimization, notice, and choice within the IoT. One participant suggested that, as part of a data minimization exercise, companies should ask themselves a series of questions, such as whether they need a particular piece of data or whether the data can be deidentified.[98] Another participant gave a specific example of how data could be minimized in the context of connected cars. This participant noted that the recording device on such cars could "automatically delete old data after a certain amount of time, or prevent individual data from being automatically synched with a central database."[99]

As to notice and choice, one auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in "[p]lain language and multiple choices of levels."[100] Another discussed a "consumer profile management portal[]" approach that would include privacy settings menus that consumers can configure and revisit,[101] possibly on a separate device such as a smartphone or a webportal. In addition to the types of specific settings and choices, another participant suggested that devices and their associated platforms could enable consumers to aggregate choices into "packets."[102] Finally, one participant noted that

---

Privacy Forum, #510 cmt. #00013, Appendix A at 4. As noted above, this report addresses privacy and security practices for consumer-facing products.

[98] Remarks of Chibba, Transcript of Workshop at 300-01.

[99] Comment of EPIC, #484 cmt. #00011 at 17-18.

[100] Remarks of Kenneth Wayne Powell, Toyota Technical Center ("Powell"), Transcript of Workshop at 278.

[101] *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

[102] Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology ("Hall"), Transcript of Workshop at 216.

companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize privacy choices.[103]

Some participants advocated for an increased focus on certain types of use restrictions to protect consumer data.[104] With this approach, legislators, regulators, self-regulatory bodies, or individual companies would set "permissible" and "impermissible" uses of certain consumer data. One commenter characterized this approach as "shifting responsibility away from data subjects toward data users, and increasing the emphasis on responsible data stewardship and accountability."[105]

Participants offered a variety of approaches to adding use-based data protections. One participant proposed that companies "tag" data with its appropriate uses so that automated processes could identify and flag inappropriate uses.[106] Other participants noted that policymakers could constrain certain uses of IoT data that do not comport with consumer expectations and present the most risk of harm, either through law[107] or through voluntary

[103] Remarks of Nguyen, Transcript of Workshop at 48.

[104] *See* Remarks of Peppet, Transcript of Workshop at 210-211 (advocating "drawing some lines around acceptable use" through legislation or regulation in addition to notice and choice); *see also* Remarks of Crosley at 213 (supporting "the appropriate use of the context"); Remarks of Hall at 214 (expressing support for "[u]se restrictions, as long as they have teeth. That's why I think vanilla self-regulatory efforts are probably not the answer. You need to have something that is enforced by an independent body").

[105] Comment of Software & Information Industry Association, #484 cmt #00025 at 8.

[106] *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 10–11 (citing Hal Abelson, *Information Accountability as the Foundation of 21st Century Privacy Protection* (2013), *available at* http://kit.mit.edu/sites/default/files/documents/Abelson_MIT_KIT_2013_Conference.pdf). We note that such an approach would require coordination and potential associated costs.

[107] *See* Peppet, *Regulating the Internet of Things*, *supra* note 62, at 149 (proposing regulatory constraints).

self-regulatory efforts[108] or seal programs.[109] For example, as one participant has pointed out, some state laws restrict access by auto insurance companies and other entities to consumers' driving data recorded by an EDR.[110]

Post-Workshop Developments

Since the November 2013 workshop, the IoT marketplace has continued to develop at a remarkable pace. For example, in June 2014, Apple announced "HealthKit," a platform that "functions as a dashboard for a number of critical metrics as well as a hub for select third-party fitness products,"[111] as a way to help protect health information that some connected devices may collect. Similarly, in October 2014, Microsoft announced Microsoft Health, a "cloud-based service that … provid[es] actionable insights based on data gathered from the fitness devices and apps" and which will work in conjunction with Microsoft's HealthVault, which for a decade has offered "a trusted place to store health information and share it with medical professionals on a security-enhanced platform."[112] And last November, Intel announced a "new platform …

[108] *See, e.g.*, *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 7; *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010 at 2; *Comment of CTIA – The Wireless Ass'n*, # 510 cmt. #00014 at 4; *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

[109] *See, e.g.*¸*Comment of AT&T Inc.*, #484 cmt. #00004 at 9–10; *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 13.

[110] Peppet, *Regulating the Internet of Things*, *supra* note 62, at 153-54.

[111] Rachel King, *Apple takes app-based approach to health tech with HealthKit*, ZDNet (June 2, 2014), *available at* http://www.zdnet.com/article/apple-takes-app-based-approach-to-health-tech-with-healthkit/.

[112] Microsoft Health, http://www.microsoft.com/Microsoft-Health/en-us (last visited Jan. 9, 2015).

designed to make it easier for developers to connect devices securely, bring device data to the cloud, and make sense of that data with analytics."[113]

Policymakers have also tried to keep pace with these developments in the IoT. For example, in May 2014, the White House released a Big Data report ("White House Big Data Report"), and the President's Council of Advisors on Science and Technology released a companion report ("PCAST Report"). Both reports weigh in on the debate between the application of data minimization, notice, and choice versus use limitations. The White House Big Data Report opined that "the notice and consent framework threatens to be overcome" in certain instances, "such as the collection of ambient data by our household appliances."[114] The White House Big Data Report concluded that,

> Putting greater emphasis on a responsible use framework has many potential advantages. It shifts the responsibility from the individual, who is not well equipped to understand or contest consent notices as they are currently structured in the marketplace, to the entities that collect, maintain, and use data. Focusing on responsible use also holds data collectors and users accountable for how they manage the data and any harms it causes, rather than narrowly defining their responsibility to whether they properly obtained consent at the time of collection.[115]

Attention to the impact of the IoT spans the globe. In September 2014, Europe's Article 29 Working Group – composed of data protection authorities of EU member countries – issued

---

[113] Aaron Tilley, Intel Releases New Platform To Kickstart Development In The Internet Of Things, FORBES (Dec. 9, 2014), *available at* http://www.forbes.com/sites/aarontilley/2014/12/09/intel-releases-new-platform-to-kickstart-development-in-the-internet-of-things/.

[114] Executive Office of the President, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES (May 2014) ("White House Big Data Report") at 56, *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf. *See also* President's Council of Advisors on Science and Technology, REPORT TO THE PRESIDENT: BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE 38 (May 2014), *available at* http://www.whitehouse.gov/administration/eop/ostp/pcast.

[115] *White House Big Data Report* at 56.

an Opinion on Recent Developments on the Internet of Things.[116] In the opinion, the Working Group emphasized the importance of user choice, noting that "users must remain in complete control of their personal data throughout the product lifecycle, and when organisations rely on consent as a basis for processing, the consent should be fully informed, freely given and specific."

In addition to policy work by government agencies, standards organizations related to the Internet of Things continue to proliferate. One such area for standard-setting is data security. For example, in August 2014, oneM2M, a global standards body, released a proposed security standard for IoT devices. The standard addresses issues such as authentication, identity management, and access control.[117]

Commission Staff's Views and Recommendations for Best Practices

This section sets forth the Commission staff's views on the issues of data security, data minimization, and notice and choice with respect to the IoT and provides recommendations for best practices for companies.

DATA SECURITY

As noted, there appeared to be widespread agreement that companies developing IoT products should implement reasonable security. Participants also discussed a number of specific security best practices. The Commission staff encourages companies to consider adopting these

[116] Article 29 Working Group Opinion, *supra* note 55.

[117] *See* oneM2M, *Technical Specification, oneM2M Security Solutions* at 15-16, *available at* http://www.onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf.

practices. Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities. Nonetheless, the specific security best practices companies should consider include the following:

First, companies should implement "security by design" by building security into their devices at the outset, rather than as an afterthought.[118] One participant stated that security should be designed into every IoT product, at every stage of development, including "early on in the design cycle of a technology."[119] In addition, a company should do a privacy or security risk assessment, consciously considering the risks presented by the collection and retention of consumer information.[120] As part of this process, companies should incorporate the use of smart defaults, such as requiring consumers to change default passwords – if they use default passwords at all – during the set-up process.[121] Companies also should consider how to minimize the data they collect and retain, as discussed further below. Finally, companies should test their security measures before launching their products. As one participant pointed out, such testing should occur because companies – and service providers they might use to help develop their

[118] *Comment of ARM and AMD*, #510 cmt. #00018 at 2; *see also* Remarks of Hagins, Transcript of Workshop at 111; Remarks of Jacobs, Transcript of Workshop at 296; Remarks of Caprio, Transcript of Workshop at 298.

[119] Remarks of Kohno, Transcript of Workshop at 281.

[120] Remarks of Chibba, Transcript of Workshop at 301; *see also* Remarks of Rogers, Transcript of Workshop at 343.

[121] *See generally* Remarks of Rogers, Transcript of Workshop at 344 ("Default passwords are something that should never pass through into production space. It's an easy thing to pick up with a very basic assessment, yet we are constantly seeing these come through because these companies aren't often doing this kind of assessment − so they see it as a hindrance, an extra step. Or they claim the consumer should be responsible for setting the security, once it lands on the consumer's desk which, at the end of the day, the consumers aren't capable of setting that level of security, nor should they have to.").

products – may simply forget to close "backdoors" in their products through which intruders could access personal information or gain control of the device.[122]

This last point was illustrated by the Commission's recent actions against the operators of the Credit Karma and Fandango mobile apps. In these cases, the companies overrode the settings provided by the Android and iOS operating systems, so that SSL encryption was not properly implemented. As a result, the Commission alleged, hackers could decrypt the sensitive consumer financial information being transmitted by the apps. The orders in both cases include provisions requiring the companies to implement reasonable security.[123]

Second, companies must ensure that their personnel practices promote good security. As part of their personnel practices, companies should ensure that product security is addressed at the appropriate level of responsibility within the organization. One participant suggested that "if someone at an executive level has responsibility for security, it tends to drive hiring and processes and mechanisms throughout the entire organization that will improve security."[124] Companies should also train their employees about good security practices, recognizing that technological expertise does not necessarily equate to security expertise. Indeed, one participant stated that being able to write software code "doesn't mean…understand[ing] anything whatsoever about the security of an embedded device."[125]

---

[122] *See generally* Remarks of Heffner, Transcript of Workshop at 73-74.

[123] Credit Karma, Inc., File No. 132-3091 (Mar. 28, 2014) (consent), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc; Fandango, LLC, File No. 132-3089 (Mar. 28, 2014) (consent), *available at* http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc. *See also* HTC America, Inc., No. C-4406 (July 2, 2013) (consent) (alleging that HTC, among other things, failed to conduct assessments, audits, reviews, or tests to identify potential security vulnerabilities in its mobile devices), *available at* http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter.

[124] Remarks of Hagins, Transcript of Workshop at 110.

[125] *Id.* at 92.

Third, companies must work to ensure that they retain service providers that are capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so. Failure to do so could result in an FTC law enforcement action. For example, in the Commission's recent settlement with GMR Transcription Services, the Commission alleged that a medical and legal transcription company outsourced transcription services to independent typists in India without adequately checking to make sure they could implement reasonable security measures. According to the Commission's complaint, among other things, the service provider stored transcribed notes in clear text on an unsecured server. As a result, U.S. consumers found their doctors' notes of their physical examinations freely available through Internet searches. This case illustrates the strong need for appropriate service provider oversight.

Fourth, for systems with significant risk, companies should implement a defense-in-depth approach, where security measures are considered at several levels. For example, participants raised concerns about relying on the security of consumers' own networks, such as passwords for their Wi-Fi routers, alone to protect the information on connected devices.[126] They noted that companies must take "additional steps to encrypt [the information] or otherwise secure it."[127] FTC staff shares these concerns and encourages companies to take additional steps to secure information passed over consumers' home networks. Indeed, encryption for sensitive information, such as that relating to health, is particularly important in this regard.[128] Regardless of the specific technology, companies should reasonably secure data in transit and in storage.

---

[126] *Id.* at 102.

[127] Remarks of Heffner, Transcript of Workshop at 102-03.

[128] Remarks of Hall, Transcript of Workshop at 178-79.

Fifth, panelists noted that companies should consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network.[129] In the IoT ecosystem, strong authentication could be used to permit or restrict IoT devices from interacting with other devices or systems. The privileges associated with the validated identity determine the permissible interactions between the IoT devices and could prevent unauthorized access and interactions.[130] In implementing these protections, companies should ensure that they do not unduly impede the usability of the device. As noted above, the proposed oneM2M security standard includes many of the recommendations discussed above.[131] Such efforts are important to the success of IoT.

Finally, companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities. Many IoT devices have a limited life cycle, resulting in a risk that consumers will be left with out-of-date IoT devices that are vulnerable to critical, publicly known security or privacy bugs. Companies may reasonably decide to limit the time during which they provide security updates and software patches, but it is important that companies weigh these decisions carefully. Companies should also be forthright in their representations about providing ongoing security updates and software patches. Disclosing the length of time companies plan to support and release software updates for a given product line will help consumers better understand the safe 'expiration dates' for their commodity Internet-

---

[129] *See, e.g.*, BRETT C. TJADEN, FUNDAMENTALS OF SECURE COMPUTER SYSTEMS 5 (2004). *See also* HP, INTERNET OF THINGS RESEARCH STUDY, *supra* note 41, at 4-5 (noting that approximately 60% of IoT devices examined had weak credentials).

[130] There may be other appropriate measures, as the security measures that a company should implement vary, depending on the risks presented by unauthorized access to the device, and the sensitivity of any information collected.

[131] oneM2M Candidate Release August 2014, *available at* http://www.onem2m.org/technical/candidate-release-august-2014 (last visited Dec. 19, 2014).

connected devices. In addition, companies that do provide ongoing support should also notify consumers of security risks and updates.

Several of these principles are illustrated by the Commission's first case involving an Internet-connected device. TRENDnet[132] marketed its Internet-connected cameras for purposes ranging from home security to baby monitoring, claiming that they were "secure." In its complaint, the Commission alleged, among other things, that the company transmitted user login credentials in clear text over the Internet, stored login credentials in clear text on users' mobile devices, and failed to test consumers' privacy settings to ensure that video feeds marked as "private" would in fact be private.[133] As a result of these alleged failures, hackers were able to access live feeds from consumers' security cameras and conduct "unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."[134] This case demonstrates the importance of practicing security-by-design.

[132] Press Release, FTC, Marketer of Internet-Connected Home Security Video Cameras Settles FTC Charges It Failed to Protect Consumers' Privacy (Sept. 4, 2013), *available at* http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles.

[133] Complaint of FTC, TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (consent), *available at* http://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf.

[134] *Id*. at 5.

Of course, the IoT encompasses a wide variety of products and services, and, as noted, the specific security measures that a company needs to implement will depend on a number of factors.[135] Devices that collect sensitive information, present physical security or safety risks (such as door locks, ovens, or insulin pumps), or connect to other devices or networks in a manner that would enable intruders to access those devices or networks should be more robustly secured than, for example, devices that simply monitor room temperatures, miles run, or calories ingested.

DATA MINIMIZATION

Commission staff agrees with workshop participants who stated that the data minimization principle remains relevant and important to the IoT.[136] While staff recognizes that companies need flexibility to innovate around new uses of data, staff believes that these interests can and should be balanced with the interests in limiting the privacy and data security risks to consumers.[137] Accordingly, companies should examine their data practices and business needs

[135] *See, e.g.*, FTC, Commission Statement Marking the FTC's 50th Data Security Settlement (Jan. 31, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf:

> The touchstone of the Commission's approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities. Through its settlements, testimony, and public statements, the Commission has made clear that it does not require perfect security; reasonable and appropriate security is a continuous process of assessing and addressing risks; there is no one-size-fits-all data security program; and the mere fact that a breach occurred does not mean that a company has violated the law.

[136] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7.

[137] *See, e.g.*, *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 3; Remarks of Chibba, Transcript of Workshop at 329–30.

and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.[138]

Data minimization is a long-standing principle of privacy protection and has been included in several policy initiatives, including the 1980 OECD Privacy Guidelines, the 2002 Asia-Pacific Economic Cooperation ("APEC") Privacy Principles, and the 2012 White House Consumer Privacy Bill of Rights.[139] Some observers have debated how data minimization would apply to new technologies.[140] In the IoT ecosystem, data minimization is challenging, but it remains important.[141] Indeed, data minimization can help guard against two privacy-related risks. First, collecting and retaining large amounts of data increases the potential harms associated with a data breach, both with respect to data stored on the device itself as well as in the cloud. Larger data stores present a more attractive target for data thieves, both outside and inside a company –

---

[138] Privacy Report, *supra* note 85, at 26–27; *see also* Mobile Disclosures Report, *supra* note 96, at 1 n.2; FTC, Data Brokers: A Call for Transparency and Accountability 55 (2014) ("Data Broker Report"), *available at* http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

[139] *See* Privacy Report, *supra* note 85, at 26–27; OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, at ¶ 7 (2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf (same); Dept. of Homeland Security, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security § 5 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (stating a Data Minimization principle: "DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)."); Exec. Office of the President, National Strategy for Trusted Identities in Cyberspace 45 (Apr. 2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf (stating a Data Minimization principle: "Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).").

[140] *See* White House Big Data Report, *supra* note 114, at 54 (Because "the logic of collecting as much data as possible is strong … focusing on controlling the collection and retention of personal data, while important, may no longer be sufficient to protect personal privacy."); PCAST Report at x-xi ("[A] policy focus on limiting data collection will not be a broadly applicable or scalable strategy – nor one likely to achieve the right balance between beneficial results and unintended negative consequences (such as inhibiting economic growth).").

[141] *See, e.g.*, Remarks of Tien, Transcript of Workshop at 107–08; *Comment of Ctr. for Democracy & Tech.*, #510 cmt. #00016 at 6–7. *See also* Article 29 Working Group Opinion, *supra* note 55, at 16–17.

and increases the potential harm from such an event.[142] Thieves cannot steal data that has been deleted after serving its purpose; nor can thieves steal data that was not collected in the first place. Indeed, in several of its data security cases, the Commission has alleged that companies could have mitigated the harm associated with a data breach by disposing of customer information they no longer had a business need to keep.[143]

Second, if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations. For example, in 2010, Commission staff sent a letter to the founders of XY magazine, a magazine for gay youth, regarding their negotiations to sell in bankruptcy customer information dating back to as early as 1996. The staff noted that, because the magazine had ceased to exist for a period of three years, the subscribers were likely to have become adults and moved on, and because continued use of their information would have been contrary to their reasonable expectations, XY should delete the personal information.[144] In this case, the risk associated with continued storage and use of the subscribers' personal information contrary to their reasonable expectations would not have existed if the company had engaged in reasonable data minimization practices.

Although these examples are not IoT-specific, they demonstrate the type of risk created by the expansive collection and retention of data. To minimize these risks, companies should

---

[142] Remarks of Chibba, Transcript of Workshop at 340; Privacy Report, *supra* note 85, at 27–29.

[143] *See CardSystems Solutions, Inc.*, No. C-4168, 2006 WL 2709787 (F.T.C. Sept. 5, 2006) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch; *DSW, Inc.*, No. C-4157, 2006 WL 752215 (F.T.C. Mar. 7, 2006) (consent order); *BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005) (consent order), *available at* http://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter. Commissioner Ohlhausen was not a commissioner at the time of these cases and therefore did not participate in them.

[144] Letter from David C. Vladeck, Dir., FTC Bureau of Consumer Prot., to Peter Larson and Martin E. Shmagin (July 1, 2010), *available at* http://www.ftc.gov/enforcement/cases-proceedings/closing-letters/letter-xy-magazine-xycom-regarding-use-sale-or.

examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.[145] Such an exercise is integral to a privacy-by-design approach and helps ensure that the company has given thought to its data collection practices on the front end by asking questions such as what types of data it is collecting, to what end, and how long it should be stored.[146] The process of mindfully considering data collection and retention policies and engaging in a data minimization exercise could also serve an education function for companies, while at the same time, protecting consumer privacy.[147]

As an example of how data minimization might work in practice, suppose a wearable device, such as a patch, can assess a consumer's skin condition. The device does not need to collect precise geolocation information in order to work; however, the device manufacturer believes that such information might be useful for a future product feature that would enable users to find treatment options in their area. As part of a data minimization exercise, the company should consider whether it should wait to collect geolocation until after it begins to offer the new product feature, at which time it could disclose the new collection and seek consent. The company should also consider whether it could offer the same feature while collecting less information, such as by collecting zip code rather than precise geolocation. If the company does decide it needs the precise geolocation information, it should provide a prominent disclosure about its collection and use of this information, and obtain consumers' affirmative

[145] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

[146] *Id. See also* Remarks of Chibba, Transcript of Workshop at 330.

[147] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 4.

express consent. Finally, it should establish reasonable retention limits for the data it does collect.

To the extent that companies decide they need to collect and maintain data to satisfy a business purpose, they should also consider whether they can do so while maintaining data in de-identified form. This may be a viable option in some contexts and helps minimize the individualized data companies have about consumers, and thus any potential consumer harm, while promoting beneficial societal uses of the information. For example, one university hospital offers a website and an associated smart phone app that collect information from consumers, including geolocation information, to enable users to find and report flu activity in their area.[148] The hospital can maintain and post information in anonymous and aggregate form, which can benefit public health authorities and the public, while at the same time maintaining consumer privacy.

A key to effective de-identification is to ensure that the data cannot be reasonably re-identified. For example, U.S. Department of Health and Human Service regulations[149] require entities covered by HIPAA to either remove certain identifiers, such as date of birth and five-digit zip code, from protected health information[150] or have an expert determine that the risk of re-identification is "very small."[151] As one participant discussed,[152] in 2009, a group of experts attempted to re-identify approximately 15,000 patient records that had been de-identified under

[148] *See* Flu Near You, *available at* https://flunearyou.org/.

[149] 45 C.F.R. §§ 164.514(a)-(c).

[150] 45 C.F.R. § 165.514(b)(2).

[151] 45 C.F.R. § 165.514(b)(1).

[152] *Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 8.

the HIPAA standard. They used commercial data sources to re-identify the data and were able to identify only 0.013% of the individuals.[153] While deidentification can be challenging in several contexts,[154] appropriately de-identified data sets that are kept securely and accompanied by strong accountability mechanisms, can reduce many privacy risks.

Of course, as technology improves, there is always a possibility that purportedly de-identified data could be re-identified.[155] This is why it is also important for companies to have accountability mechanisms in place. When a company states that it maintains de-identified or anonymous data, the Commission has stated that companies should (1) take reasonable steps to de-identify the data, including by keeping up with technological developments; (2) publicly commit not to re-identify the data; and (3) have enforceable contracts in place with any third parties with whom they share the data, requiring the third parties to commit not to re-identify the data.[156] This approach ensures that if the data is not reasonably de-identified and then is re-identified in the future, regulators can hold the company responsible.

With these recommendations on data minimization, Commission staff is mindful of the need to balance future, beneficial uses of data with privacy protection. For this reason, staff's recommendation is a flexible one that gives companies many options: they can decide not to

---

[153] *Id.*

[154] Technical experts continue to evaluate the effectiveness of deidentification for different types of data, and some urge caution in interpreting claims about the effectiveness of specific technical means of deidentification. *See, e.g.*, Arvind Narayanan and Edward Felten, No Silver Bullet: De-Identification Still Doesn't Work (July 9, 2014), *available at* http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf.

[155] *See, e.g.*, Ann Cavoukian and Khaled El Emam, De-identification Protocols: Essential for Protecting Privacy (June 25, 2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/06/pbd-de-identifcation_essential.pdf; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 8; Privacy Report, *supra* note 85, at 21.

[156] *See* Privacy Report, *supra* note 85, at 21; *see also Comment of Future of Privacy Forum*, #510 cmt. #00013, Appendix A at 7.

collect data at all; collect only the fields of data necessary to the product or service being offered; collect data that is less sensitive; or de-identify the data they collect. If a company determines that none of these options work, it can seek consumers' consent for collecting additional, unexpected data. In addition, in considering reasonable collection and retention limits, it is appropriate to consider the sensitivity of the data at issue: the more sensitive the data, the more harmful it could be if the data fell into the wrong hands or were used for purposes the consumer would not expect. Through this approach, a company can minimize its data collection, consistent with its business goals.[157] As one participant noted, "[p]rotecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and privacy by design."[158]

NOTICE AND CHOICE

While the traditional methods of providing consumers with disclosures and choices may need to be modified as new business models continue to emerge, staff believes that providing notice and choice remains important, as potential privacy and security risks may be heightened due to the pervasiveness of data collection inherent in the IoT. Notice and choice is particularly important when sensitive data is collected.[159]

---

[157] *See, e.g.*, *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 10 (describing its Smart Grid privacy seal).

[158] *Comment of Transatl. Computing Continuum Policy Alliance*, #484 cmt. #00021 at 3. *See also* Remarks of Chibba, Transcript of Workshop at 330.

[159] *See, e.g.*, *Comment of Future of Privacy Forum*, #510 cmt. #00013 at 6 ("In some cases, however, such as when consumers are purchasing connected devices that will collect personally identifiable health information, the presentation of privacy policies will be important to helping consumers make informed choices."); *Comment of Ctr. for Digital Democracy*, #484 cmt. #00006 at 3 ("[T]he combined impact of the mobile marketing and real-time data revolution and the Internet of Things places consumer privacy at greater risk than ever before.").

Moreover, staff believes that providing consumers with the ability to make informed choices remains practicable in the IoT. This does not mean that every data collection requires choice. The Commission has recognized that providing choices for every instance of data collection is not necessary to protect privacy. In its 2012 Privacy Report, which set forth recommended best practices, the Commission stated that companies should not be compelled to provide choice before collecting and using consumer data for practices that are consistent with the context of a transaction or the company's relationship with the consumer. Indeed, because these data uses are generally consistent with consumers' reasonable expectations, the cost to consumers and businesses of providing notice and choice likely outweighs the benefits.[160] This principle applies equally to the Internet of Things.

For example, suppose a consumer buys a smart oven from ABC Vending, which is connected to an ABC Vending app that allows the consumer to remotely turn the oven on to the setting, "Bake at 400 degrees for one hour." If ABC Vending decides to use the consumer's oven-usage information to improve the sensitivity of its temperature sensor or to recommend another of its products to the consumer, it need not offer the consumer a choice for these uses, which are consistent with its relationship with the consumer. On the other hand, if the oven manufacturer shares a consumer's personal data with, for example, a data broker or an ad network, such sharing would be inconsistent with the context of the consumer's relationship with the manufacturer, and the company should give the consumer a choice. The practice of distinguishing contextually appropriate data practices from those that are inconsistent with

[160] Privacy Report, *supra* note 85, at 38-39; *id.* at 38 ("The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary.").

context reduces the need for companies to provide opportunities for consumer choice before every single data collection.

Staff acknowledges the practical difficulty of providing choice when there is no consumer interface, and recognizes that there is no one-size-fits-all approach. Some options – several of which were discussed by workshop participants – include the following:

- **Choices at point of sale:**
  One auto industry participant noted that his company provides consumers with opt-in choices at the time of purchase in "[p]lain language and multiple choices of levels."[161]

- **Tutorials:**
  Facebook offers a video tutorial to guide consumers through its privacy settings page. IoT device manufacturers can offer similar vehicles for explaining and providing choices to consumers.

- **Codes on the device:**
  Manufacturers could affix a QR code or similar barcode that, when scanned, would take the consumer to a website with information about the applicable data practices and enable consumers to make choices through the website interface.[162]

- **Choices during set-up:**
  Many IoT devices have an initial set-up wizard, through which companies could provide clear, prominent, and contextual privacy choices.

[161] Remarks of Kenneth Wayne Powell, Toyota Technical Center ("Powell"), Transcript of Workshop at 278.

[162] *See* Article 29 Working Group Opinion, *supra* note 55, at 18 (proposing that a "device manufacturer could print on things equipped with sensors a QR code, or a flashcode describing the type of sensors and the information it captures as well as the purposes of these data collections").

- **Management portals or dashboards:**[163]
  In addition to the availability of initial set-up choices, IoT devices could also include privacy settings menus that consumers can configure and revisit. For example, in the mobile context, both Apple and Google (for Android) have developed dashboard approaches that seem promising – one that is framed by data elements, such as geolocation and contacts (Apple), and one that is framed by individual apps (Android).[164] Similarly, companies developing "command centers" for their connected home devices[165] could incorporate similar privacy dashboards. Properly implemented, such "dashboard" approaches can allow consumers clear ways to determine what information they agree to share.

- **Icons:**
  Devices can use icons to quickly convey important settings and attributes, such as when a device is connected to the Internet, with a toggle for turning the connection on or off.

- **"Out of Band" communications requested by consumers:**
  When display or user attention is limited, it is possible to communicate important privacy and security settings to the user via other channels. For example, some home appliances allow users to configure their devices so that they receive important information through emails or texts.

- **General Privacy Menus:**
  In addition to the types of specific settings and choices described above, devices and their associated platforms could enable consumers to aggregate choices into "packets." [166] This could involve having more general settings like "low privacy," "medium," or "high," accompanied by a clear and conspicuous explanation of the settings.

- **A User Experience Approach:**
  One participant noted that companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize choices.[167] For example, a manufacturer that offers two or more devices could use the consumer's preferences on one device (*e.g.*, "do not transmit any of my information to third parties") to set a default preference on another. As another example, a single device, such as a home appliance "hub" that stores data locally – say on the consumer's home network – could learn a consumer's preferences based on prior behavior and predict future privacy preferences as new appliances are added to the hub.

---

[163] *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 6.

[164] *See* Mobile Disclosures Report, *supra* note 96, at 16-17.

[165] Don Clark, *The Race to Build Command Centers for Smart Homes*, WALL ST. J. (Jan. 4, 2015), *available at* http://www.wsj.com/articles/the-race-to-build-command-centers-for-smart-homes-1420399511.

[166] Remarks of Joseph Lorenzo Hall, Center for Democracy & Technology ("Hall"), Transcript of Workshop at 216.

[167] Remarks of Nguyen, Transcript of Workshop at 48.

Of course, whatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents.[168] In addition, companies may want to consider using a combination of approaches.

Staff also recognizes concerns discussed at the workshop[169] and, as noted above, in the White House Big Data Report and PCAST Report that, applied aggressively, a notice and choice approach could restrict unexpected new uses of data with potential societal benefits. For this reason, staff has incorporated certain elements of the use-based model into its approach. For instance, the idea of choices being keyed to context takes into account how the data will be used: if a use is consistent with the context of the interaction – in other words, it is an expected use – then a company need not offer a choice to the consumer. For uses that would be inconsistent with the context of the interaction (*i.e.*, unexpected), companies should offer clear and conspicuous choices. Companies should not collect sensitive data without affirmative express consent.

In addition, if a company enables the collection of consumers' data and de-identifies that data immediately and effectively, it need not offer choices to consumers about this collection. As noted above, robust de-identification measures can enable companies to analyze data they collect in order to innovate in a privacy-protective way.[170] Companies can use such de-identified data without having to offer consumers choices.

---

[168] This discussion refers to how companies should communicate choices to consumers. Lengthy privacy policies are not the most effective consumer communication tool. However, providing disclosures and choices through these privacy policies serves an important accountability function, so that regulators, advocacy groups, and some consumers can understand and compare company practices and educate the public. *See* Privacy Report, *supra* note 85, at 61-64.

[169] *See, e.g., Comment of Future of Privacy Forum*, #510 cmt. #00013, App. A at 9; *Comment of GS1 US*, #484 cmt. #00030 at 5; *Comment of Software & Info. Indus. Ass'n.*, #484 cmt. #00025 at 6-9.

[170] *See, e.g.*, Comment of CTIA – The Wireless Ass'n, #484 cmt. #00009 at 10-11; Comment of Future of Privacy Forum, #510 cmt. #00013 at 5.

Staff also notes that existing laws containing elements of the use-based approach apply to the IoT. The FCRA sets forth a number of statutory protections applicable to "consumer report" information, including restrictions on the uses for which this information can be shared.[171] Even when there is a permissible use for such information, the FCRA imposes an array of protections, including those relating to notice, access, disputes, and accuracy.[172] In addition, the FTC has used its "unfairness" authority to challenge a number of harmful uses of consumer data. For example, in the agency's recent case against Leap Lab, the Commission alleged that defendants sold consumer payday loan applications that included consumers' Social Security and financial account numbers to non-lenders that had no legitimate need for this sensitive personal information.[173]

Staff has concerns, however, about adopting solely a use-based model for the Internet of Things. First, because use-based limitations have not been fully articulated in legislation or other widely-accepted multistakeholder codes of conduct, it is unclear who would decide which additional uses are beneficial or harmful.[174] If a company decides that a particular data use is beneficial and consumers disagree with that decision, this may erode consumer trust. For example, there was considerable consumer outcry over Facebook's launch of the Beacon service,

---

[171] FCRA, 15 U.S.C. § 1681–1681v. Section 604 of the FCRA sets forth the permissible purposes for which a consumer reporting company may furnish consumer report information, such as to extend credit or insurance or for employment purposes. 15 U.S.C. 1681b.

[172] FCRA, 15 U.S.C. § 1681–1681v.

[173] Press Release, FTC, FTC Charges Data Broker with Facilitating the Theft of Millions of Dollars from Consumers' Accounts (Dec. 23, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/12/ftc-charges-data-broker-facilitating-theft-millions-dollars.

[174] ANN CAVOUKIAN ET AL., INFO. & PRIVACY COMM'R, ONT., CAN., THE UNINTENDED CONSEQUENCES OF PRIVACY PATERNALISM (2014), *available at* http://www.privacybydesign.ca/content/uploads/2014/03/pbd-privacy_paternalism.pdf.

as well as Google's launch of the Buzz social network, which ultimately led to an FTC enforcement action.[175]

Second, use limitations alone do not address the privacy and security risks created by expansive data collection and retention. As explained above, keeping vast amounts of data can increase a company's attractiveness as a data breach target, as well as the risk of harm associated with any such data breach. For this reason, staff believes that companies should seek to reasonably limit the data they collect and dispose of it when it is no longer needed.

Finally, a use-based model would not take into account concerns about the practice of collecting sensitive information.[176] Consumers would likely want to know, for example, if a company is collecting health information or making inferences about their health conditions, even if the company ultimately does not use the information.[177]

---

[175] *See, e.g.*, Google Inc., No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf.

[176] In addition to collecting sensitive information outright, companies might create sensitive information about consumers by making inferences from other data that they or others have already collected. A use-based model might not address, or provide meaningful notice about, sensitive inferences. The extent to which a use-based model limits or prohibits sensitive inferences will depend on how the model defines harms and benefits and how it balances the two, among other factors.

[177] Of course, if a company misstates how it uses data, this could be a deceptive practice under Section 5 of the FTC Act. The FTC has brought cases against companies that promise to use consumers' data one way, but used it in another way. *See, e.g.*, Google Inc., *supra* note 175. The FTC can also use its unfairness authority to prohibit uses of data that cause or are likely to cause substantial injury to a consumer, where that injury was not reasonably avoidable by the consumer, and where the injury was not outweighed by a benefit to consumers or competition. *See, e.g.*, Designerware, LLC, No. C-4390 (Apr. 11, 2013) (consent order) (alleging that installing and turning on webcams on people's home computers without their knowledge or consent was an unfair practice), *available at* http://www.ftc.gov/enforcement/cases-proceedings/112-3151/designerware-llc-matter.

The establishment of legislative or widely-accepted multistakeholder use-based frameworks could potentially address some of these concerns and should be considered. For example, the framework could set forth permitted or prohibited uses. In the absence of such legislative or widely accepted multistakeholder frameworks, however, the approach set forth here – giving consumers information and choices about their data – continues to be the most viable one for the IoT in the foreseeable future.

Legislation

Summary of Workshop Discussions

Workshop participants discussed whether legislation is needed to ensure appropriate protections for data collected through connected devices. Some participants expressed trepidation that the benefits of the IoT might be adversely affected should policymakers enact laws or regulations on industry.[178] One participant stated, "[t]he FTC should be very cautious about proposing regulation of this sector, given its importance to innovation in America."[179] Another participant noted that "we should be careful to kind of strike a balance between guiding companies in the right direction and enforcing."[180] Still another worried that the workshop might "represent[] the beginning of a regulatory regime for a new set of information technologies that are still in their infancy" and advised policymakers to "exercise restraint and avoid the impulse to regulate before serious harms are demonstrated."[181] Another participant questioned what legislation would look like, given the difficulty of defining the contours of privacy rights.[182]

A number of participants noted that self-regulation is the appropriate approach to take to the IoT. One participant stated, "self-regulation and best business practices – that are technology

[178] *See, e.g.*, *Comment of Direct Mktg. Ass'n*, #484 cmt. #00010.

[179] *Comment of Internet Commerce Coal.*, #484 cmt. #00020 at 2.

[180] Remarks of Rogers, Transcript of Workshop at 359.

[181] *Comment of Tech. Policy Program of the Mercatus Ctr., George Mason Univ.*, #484 cmt. #00024 at 1 and 9.

[182] Remarks of Cerf, Transcript of Workshop at 149-50 ("Well, I have to tell you that regulation is tricky. And I don't know, if somebody asked me, would you write a regulation for this, I would not know what to say. I don't think I have enough understanding of all of the cases that might arise in order to say something useful about this, which is why I believe we are going to end up having to experience problems before we understand the nature of the problems and maybe even the nature of the solutions.").

neutral – along with consumer education serve as the preferred framework for protecting consumer privacy and security while enhancing innovation, investment, competition, and the free flow of information essential to the Internet of Things."[183] Another participant agreed, stating "[s]elf-regulatory regimes have worked well to ensure consumer privacy and foster innovation, and industry has a strong track record of developing and implementing best practices to protect information security."[184]

Other participants noted that the time is ripe for legislation, either specific to the IoT or more generally.[185] One participant who called for legislation noted that the "explosion of fitness and health monitoring devices is no doubt highly beneficial to public health and worth encouraging," but went on to state:

> At the same time, data from these Internet of Things devices should not be usable by insurers to set health, life, car, or other premiums. Nor should these data migrate into employment decisions, credit decisions, housing decisions, or other areas of public life. To aid the development of the Internet of Things—and reap the potential public health benefits these devices can create—we should reassure the public that their health data will not be used to draw unexpected inferences or incorporated into economic decisionmaking.[186]

Recommendations

The Commission staff recognizes that this industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees with those commenters who stated that there is

---

[183] *Comment of U.S. Chamber of Commerce*, #510 cmt. #00011 at 3.

[184] *Comment of Consumer Elec. Ass'n*, #484 cmt. #00027 at 18.

[185] Remarks of Hall, Transcript of Workshop at 180-81 (supporting baseline privacy legislation); *see also* Remarks of Jacobs, Transcript of Workshop at 360 (emphasizing importance of enforcement "in the meantime").

[186] Peppet, *Regulating the Internet of Things*, *supra* note 62, at 151.

great potential for innovation in this area, and that legislation aimed specifically at the IoT at this stage would be premature. Staff also agrees that development of self-regulatory programs[187] designed for particular industries would be helpful as a means to encourage the adoption of privacy- and security-sensitive practices.

However, while IoT specific-legislation is not needed, the workshop provided further evidence that Congress should enact general data security legislation. As noted above, there was wide agreement among workshop participants about the importance of securing Internet-enabled devices, with some participants stating that many devices now available in the market are not reasonably secure, posing risks to the information that they collect and transmit and also to information on consumers' networks or even to others on the Internet.[188] These problems highlight the need for substantive data security and breach notification legislation at the federal level.

The Commission has continued to recommend that Congress enact strong, flexible, and technology-neutral legislation to strengthen the Commission's existing data security enforcement tools and require companies to notify consumers when there is a security breach. Reasonable and appropriate security practices are critical to addressing the problem of data breaches and protecting consumers from identity theft and other harms. Notifying consumers of breaches after they occur helps consumers protect themselves from any harm that is likely to be caused by the misuse of their data. These principles apply equally to the IoT ecosystem.[189]

---

[187] Remarks of Lightner, Transcript of Workshop at 56-57 (discussing voluntary code of conduct for energy data); *Comment of Future of Privacy Forum*, #484 cmt. #00013 (discussing self-regulatory efforts in a variety of contexts).

[188] *See* discussion *supra* pp. 10-14 and accompanying notes.

[189] One commenter argued that breach notification laws should be even broader in the IoT context. *See* Remarks of Peppet, Transcript of Workshop at 220 (urging that breach notification laws be extended for the IoT to cover additional types of information that would lead to consumer harm but would not meet the definition of personal

We emphasize that general technology-neutral data security legislation should protect against unauthorized access to both personal information and device functionality itself. The security risks associated with IoT devices, which are often not limited to the compromise of personal information but also implicate broader health and safety concerns, illustrate the importance of these protections. For example, if a pacemaker is not properly secured, the concern is not merely that health information could be compromised, but also that a person wearing it could be seriously harmed.[190] Similarly, a criminal who hacks into a car's network could cause a car crash. Accordingly, general data security legislation should address risks to both personal information and device functionality.

In addition, the pervasiveness of information collection and use that the IoT makes possible reinforces the need for baseline privacy standards.[191] Commission staff thus again recommends that Congress consider enacting broad-based (as opposed to IoT-specific) privacy legislation. Such legislation should be flexible and technology-neutral, while also providing clear rules of the road for companies about such issues as when to provide privacy notices to consumers and offer them choices about data collection and use practices. Although the Commission currently has authority to take action against some IoT-related practices, it cannot

---

information protected under existing laws). The Commission has not taken a position on such an approach at this time.

[190] Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/.

[191] Commissioner Ohlhausen disagrees with this portion of the staff's recommendation. She believes that the FTC's current Section 5 authority to prohibit unfair and deceptive acts or practices already requires notice and choice for collecting sensitive personally identifiable information and protects against uses of consumer information that cause or are likely to cause substantial consumer harm not outweighed by benefits to consumers or competition. Furthermore, the FCRA, HIPAA, and other laws already provide additional sector-specific privacy protections. Thus, Commissioner Ohlhausen questions what harms baseline privacy legislation would reach that the FTC's existing authority cannot.

mandate certain basic privacy protections – such as privacy disclosures or consumer choice – absent a specific showing of deception or unfairness.

The Commission has issued a report and testified before Congress calling for baseline federal privacy legislation.[192] These recommendations have been based on concerns about the lack of transparency regarding some companies' data practices and the lack of meaningful consumer control of personal data. These concerns permeate the IoT space, given the ubiquity of information collection, the broad range of uses that the IoT makes possible, the multitude of companies involved in collecting and using information, and the sensitivity of some of the data at issue.

Staff believes such legislation will help build trust in new technologies that rely on consumer data, such as the IoT. Consumers are more likely to buy connected devices if they feel that their information is adequately protected.[193] A 2012 survey shows, for example, that a majority of consumers uninstalled an app because they were concerned that it was collecting too much personal information, or declined to install an app at all.[194] A 2014 survey shows that 87% of consumers are concerned about the type of data collected through smart devices, and 88% of

---

[192] *See, e.g.*, Privacy Report, *supra* note 85, at 12-13; *The Need for Privacy Protections: Perspectives from the Administration and the Federal Trade Commission Before the S. Comm. On Commerce, Science & Transportation* (May 9, 2012) (statement of FTC), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-need-privacy-protections-perspectives-administration-and/120509privacyprotections.pdf.

[193] Remarks of Chibba, Transcript of Workshop at 312-13; *see also* Remarks of Wolf, Transcript of Workshop at 260 (noting that "the Michigan Department of Transportation and the Center for Automotive Research identified security as the primary concern for connected car technologies"); *Comment of Future of Privacy Forum*, #484 cmt. #00013 at 5 ("If there are lax controls and insufficient oversight over the collection of personal information through connected devices, consumers will lose trust in the evolving technologies. Even with proper controls and oversight, helping consumers understand the benefits from these innovations and the protections in place is important lest they feel that personal control has been sacrificed for corporate gain.").

[194] JAN LAUREN BOYLES ET AL., PEW INTERNET PROJECT, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_MobilePrivacyManagement.pdf.

consumers want to control the data that is collected through smart devices.[195] Surveys also show that consumers are more likely to trust companies that provide them with transparency and choices.[196] General privacy legislation that provides for greater transparency and choices could help both consumers and businesses by promoting trust in the burgeoning IoT marketplace.

In addition, as demonstrated at the workshop, general privacy legislation could ensure that consumers' data is protected, regardless of who is asking for it. For example, workshop participants discussed the fact that HIPAA protects sensitive health information, such as medical diagnoses, names of medications, and health conditions, but only if it is collected by certain entities, such as a doctor's office or insurance company.[197] Increasingly, however, health apps are collecting this same information through consumer-facing products, to which HIPAA protections do not apply. Commission staff believes that consumers should have transparency and choices over their sensitive health information, regardless of who collects it. Consistent standards would also level the playing field for businesses.

---

[195] The TRUSTe Internet of Things Privacy Index, 2014 U.S. Edition, *available at* http://www.truste.com/us-internet-of-things-index-2014/.

[196] *See, e.g.*, Adam DeMartino, Evidon, *RESEARCH: Consumers Feel Better About Brands that Give Them Transparency and Control Over Ads* (Nov. 10, 2010), *available at* http://www.evidon.com/blog/research-consumers-feel-better-about-brands-that-give-them-transparency-and-control-over-ads; Scott Meyer, *Data Transparency Builds Trust*, BRANDREPUBLIC (Oct. 31, 2012), *available at* http://www.brandrepublic.com/news/1157134/; TRUSTe, *New TRUSTe Survey Finds Consumer Education and Transparency Vital for Sustainable Growth and Success of Online Behavioral Advertising* (July 25, 2011), *available at* http://www.truste.com/about-TRUSTe/press-room/news_truste_behavioral_advertising_survey_2011.

[197] Remarks of Hall, Transcript of Workshop at 179; Remarks of T. Drew Hickerson, Happtique, Transcript of Workshop at 350; *Comment of Ctr. for Democracy & Tech*, #510 cmt. #00016 at 12.

While Commission staff encourages Congress to consider privacy and security legislation, we will continue to use our existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices and services. Specifically, we will engage in the following initiatives:

- **Law enforcement:**
  The Commission enforces the FTC Act, the FCRA, the Children's Online Privacy Protection Act, the health breach notification provisions of the HI-TECH Act, and other laws that might apply to the IoT. Where appropriate, staff will recommend that the Commission use its authority to take action against any actors it has reason to believe are in violation of these laws. The TRENDNet case, discussed above, was the Commission's first IoT case. We will continue to look for cases involving companies making IoT devices that, among other things, do not maintain reasonable security, make misrepresentations about their privacy practices, or violate the requirements of the FCRA when they use information for credit, employment, insurance, or other eligibility decisions. Staff believes that a strong FTC law enforcement presence will help incentivize appropriate privacy and security-protective practices by companies manufacturing and selling connected devices.

- **Consumer and business education:**
  Consumers should understand how to get more information about the privacy of their IoT devices, how to secure their home networks that connect to IoT devices, and how to use any available privacy settings. Businesses, and in particular small businesses, would benefit from additional information about how to reasonably secure IoT devices. The Commission staff will develop new consumer and business education materials in this area.

- **Participation in multi-stakeholder groups:**
  Currently, Commission staff is working with a variety of groups that are considering guidelines related to the Internet of Things. For example, staff participates in NTIA's multi-stakeholder group that is considering guidelines for facial recognition and the Department of Energy's multi-stakeholder effort to develop guidelines for smart meters. Even in the absence of legislation, these efforts can result in best practices for companies developing connected devices, which can significantly benefit consumers. Commission staff will continue to participate in multistakeholder groups to develop guidelines related to the IoT.

- **Advocacy:**
  Finally, where appropriate, the Commission staff will look for advocacy opportunities with other agencies, state legislatures, and courts to promote protections in this area. Among other things, staff will share the best practices discussed in this report with other government entities in order to ensure that they consider privacy and security issues.

Conclusion

The IoT presents numerous benefits to consumers, and has the potential to change the ways that consumers interact with technology in fundamental ways. In the future, the Internet of Things is likely to meld the virtual and physical worlds together in ways that are currently difficult to comprehend. From a security and privacy perspective, the predicted pervasive introduction of sensors and devices into currently intimate spaces – such as the home, the car, and with wearables and ingestibles, even the body – poses particular challenges. As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation.

Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

FTC REPORT

FEDERAL TRADE COMMISSION | MARCH 2012

Protecting Consumer Privacy in an Era of Rapid Change

RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS

FTC REPORT
MARCH 2012

CONTENTS

EXECUTIVE SUMMARY

In today's world of smart phones, smart grids, and smart cars, companies are collecting, storing, and sharing more information about consumers than ever before. Although companies use this information to innovate and deliver better products and services to consumers, they should not do so at the expense of consumer privacy.

With this Report, the Commission calls on companies to act now to implement best practices to protect consumers' private information. These best practices include making privacy the "default setting" for commercial data practices and giving consumers greater control over the collection and use of their personal data through simplified choices and increased transparency. Implementing these best practices will enhance trust and stimulate commerce.

This Report follows a preliminary staff report that the Federal Trade Commission ("FTC" or "Commission") issued in December 2010. The preliminary report proposed a framework for protecting consumer privacy in the 21st Century. Like this Report, the framework urged companies to adopt the following practices, consistent with the Fair Information Practice Principles first articulated almost 40 years ago:

- **Privacy by Design:** Build in privacy at every stage of product development;
- **Simplified Choice for Businesses and Consumers:** Give consumers the ability to make decisions about their data at a relevant time and context, including through a Do Not Track mechanism, while reducing the burden on businesses of providing unnecessary choices; and
- **Greater Transparency:** Make information collection and use practices transparent.

The Commission received more than 450 public comments in response to the preliminary report from various stakeholders, including businesses, privacy advocates, technologists and individual consumers. A wide range of stakeholders, including industry, supported the principles underlying the framework, and many companies said they were already following them. At the same time, many commenters criticized the slow pace of self-regulation, and argued that it is time for Congress to enact baseline privacy legislation. In this Report, the Commission addresses the comments and sets forth a revised, final privacy framework that adheres to, but also clarifies and fine-tunes, the basic principles laid out in the preliminary report.

Since the Commission issued the preliminary staff report, Congress has introduced both general privacy bills and more focused bills, including ones addressing Do Not Track and the privacy of teens. Industry has made some progress in certain areas, most notably, in responding to the preliminary report's call for Do Not Track. In other areas, however, industry progress has been far slower. Thus, overall, consumers do not yet enjoy the privacy protections proposed in the preliminary staff report.

The Administration and certain Members of Congress have called for enactment of baseline privacy legislation. The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

The remainder of this Executive Summary describes key developments since the issuance of the preliminary report, discusses the most significant revisions to the proposed framework, and lays out several next steps.

DEVELOPMENTS SINCE ISSUANCE OF THE PRELIMINARY REPORT

In the last 40 years, the Commission has taken numerous actions to shape the consumer privacy landscape. For example, the Commission has sued dozens of companies that broke their privacy and security promises, scores of telemarketers that called consumers on the Do Not Call registry, and more than a hundred scammers peddling unwanted spam and spyware. Since it issued the initial staff report, the Commission has redoubled its efforts to protect consumer privacy, including through law enforcement, policy advocacy, and consumer and business education. It has also vigorously promoted self-regulatory efforts.

On the law enforcement front, since December 2010, the Commission:

- Brought enforcement actions against Google and Facebook. The orders obtained in these cases require the companies to obtain consumers' affirmative express consent before materially changing certain of their data practices and to adopt strong, company-wide privacy programs that outside auditors will assess for 20 years. These orders will protect the more than one billion Google and Facebook users worldwide.
- Brought enforcement actions against online advertising networks that failed to honor opt outs. The orders in these cases are designed to ensure that when consumers choose to opt out of tracking by advertisers, their choice is effective.
- Brought enforcement actions against mobile applications that violated the Children's Online Privacy Protection Act as well as applications that set default privacy settings in a way that caused consumers to unwittingly share their personal data.
- Brought enforcement actions against entities that sold consumer lists to marketers in violation of the Fair Credit Reporting Act.
- Brought actions against companies for failure to maintain reasonable data security.

On the policy front, since December 2010, the FTC and staff:

- Hosted two privacy-related workshops, one on child identity theft and one on the privacy implications of facial recognition technology.
- Testified before Congress ten times on privacy and data security issues.
- Consulted with other federal agencies, including the Federal Communications Commission, the Department of Health and Human Services, and the Department of Commerce, on their privacy initiatives. The Commission has supported the Department of Commerce's initiative to convene stakeholders to develop privacy-related codes of conduct for different industry sectors.
- Released a survey of data collection disclosures by mobile applications directed to children.
- Proposed amendments to the Children's Online Privacy Protection Act Rule.

On the education front, since December 2010, the Commission:

- Continued outreach efforts through the FTC's consumer online safety portal, OnGuardOnline.gov, which provides information in a variety of formats – articles, games, quizzes, and videos – to help consumers secure their computers and protect their personal information. It attracts approximately 100,000 unique visitors per month.
- Published new consumer education materials on identity theft, Wi-Fi hot spots, cookies, and mobile devices.
- Sent warning letters to marketers of mobile apps that do background checks on individuals, educating them about the requirements of the Fair Credit Reporting Act.

To promote self-regulation, since December 2010, the Commission:

- Continued its call for improved privacy disclosures and choices, particularly in the area of online behavioral tracking. In response to this call, as well as to Congressional interest:
  - A number of Internet browser vendors developed browser-based tools for consumers to request that websites not track their online activities.
  - The World Wide Web Consortium, an Internet standard setting organization, is developing a universal web protocol for Do Not Track.
  - The Digital Advertising Alliance ("DAA"), a coalition of media and marketing organizations, has developed a mechanism, accessed through an icon that consumers can click, to obtain information about and opt out of online behavioral advertising. Additionally, the DAA has committed to preventing the use of consumers' data for secondary purposes like credit and employment and honoring the choices about tracking that consumers make through the settings on their browsers.
- Participated in the development of enforceable cross-border privacy rules for businesses to harmonize and enhance privacy protection of consumer data that moves between member countries of the forum on Asia Pacific Economic Cooperation.

THE FINAL REPORT

Based upon its analysis of the comments filed on the proposed privacy framework, as well as commercial and technological developments, the Commission is issuing this final Report. The final framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC. While retaining the proposed framework's fundamental best practices of privacy by design, simplified choice, and greater transparency, the Commission makes revised recommendations in three key areas in response to the comments.

First, the Commission makes changes to the framework's scope. The preliminary report proposed that the privacy framework apply to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device. To address concerns about undue burdens on small businesses, the final framework does not apply to companies that collect only non-sensitive data from fewer than 5,000 consumers a year, provided they do not share the data with third parties. Commenters also expressed concern that, with improvements in technology and the ubiquity of public information, more and more data could be "reasonably linked" to a consumer, computer or device, and that the proposed framework provided less incentive for a business to try to de-identify the data it maintains. To address this issue, the Report clarifies that data is not "reasonably linkable" to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.

Second, the Commission revises its approach to how companies should provide consumers with privacy choices. To simplify choice for both consumers and businesses, the proposed framework set forth a list of five categories of "commonly accepted" information collection and use practices for which companies need not provide consumers with choice (product fulfillment, internal operations, fraud prevention, legal compliance and public purpose, and first-party marketing). Several business commenters expressed concern that setting these "commonly accepted practices" in stone would stifle innovation. Other commenters expressed the concern that the "commonly accepted practices" delineated in the proposed framework were too broad and would allow a variety of practices to take place without consumer consent.

In response to these concerns, the Commission sets forth a modified approach that focuses on the context of the consumer's interaction with the business. Under this approach, companies do not need to provide choice before collecting and using consumers' data for practices that are consistent with the context of the transaction, consistent with the company's relationship with the consumer, or as required or specifically authorized by law. Although many of the five "commonly accepted practices" identified in the preliminary report would generally meet this standard, there may be exceptions. The Report provides examples of how this new "context of the interaction" standard would apply in various circumstances.

Third, the Commission recommends that Congress consider enacting targeted legislation to provide greater transparency for, and control over, the practices of information brokers. The proposed framework recommended that companies provide consumers with reasonable access to the data the companies maintain about them, proportionate to the sensitivity of the data and the nature of its use. Several commenters discussed in particular the importance of consumers' ability to access information that information brokers have about them. These commenters noted the lack of transparency about the practices of information brokers, who often buy, compile, and sell a wealth of highly personal information about consumers but never interact directly with them. Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.

The Commission agrees that consumers should have more control over the practices of information brokers and believes that appropriate legislation could help address this goal. Any such legislation could be

modeled on a bill that the House passed on a bipartisan basis during the 111th Congress, which included a procedure for consumers to access and dispute personal data held by information brokers.

IMPLEMENTATION OF THE PRIVACY FRAMEWORK

While Congress considers privacy legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission's final privacy framework. Although some companies have excellent privacy and data security practices, industry as a whole must do better. Over the course of the next year, Commission staff will promote the framework's implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the Digital Advertising Alliance ("DAA") has developed its own icon-based tool and has committed to honor the browser tools; and the World Wide Web Consortium ("W3C") has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.
- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media seek, to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

- **Promoting Enforceable Self-Regulatory Codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

FINAL FTC PRIVACY FRAMEWORK AND IMPLEMENTATION RECOMMENDATIONS

The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

SCOPE

Final Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.

PRIVACY BY DESIGN

Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

A. The Substantive Principles

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

B. Procedural Protections to Implement the Substantive Principles

Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

A. Practices That Do Not Require Choice

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.

To balance the desire for flexibility with the need to limit the types of practices for which choice is not required, the Commission has refined the final framework so that companies engaged in practices consistent with the context of their interaction with consumers need not provide choices for those practices.

B. Companies Should Provide Consumer Choice for Other Practices

Final Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

The Commission commends industry's efforts to improve consumer control over online behavioral tracking by developing a Do Not Track mechanism, and encourages continued improvements and full implementation of those mechanisms.

TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

A. Privacy notices

Final Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

B. Access

Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

The Commission has amplified its support for this principle by including specific recommendations governing the practices of information brokers.

C. Consumer Education

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

LEGISLATIVE RECOMMENDATIONS

The Commission now also calls on Congress to consider enacting baseline privacy legislation and reiterates its call for data security and data broker legislation. The Commission is prepared to work with Congress and other stakeholders to craft such legislation. At the same time, the Commission urges industry to accelerate the pace of self-regulation.

FTC WILL ASSIST WITH IMPLEMENTATION IN FIVE KEY AREAS

As discussed throughout the Commission's final Report, there are a number of specific areas where policy makers have a role in assisting with the implementation of the self-regulatory principles that make up the final privacy framework. Areas where the FTC will be active over the course of the next year include the following:

1. Do Not Track

Industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.

2. Mobile

The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures. As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

3. Data Brokers

To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker. To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.

4. Large Platform Providers

To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.

5. Promoting Enforceable Self-Regulatory Codes

The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

In all other areas, the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the final privacy framework, to the extent they have not already done so. For its part, the FTC will focus its policy efforts on the five areas identified above, vigorously enforce existing laws, work with industry on self-regulation, and continue to target its education efforts on building awareness of existing data collection and use practices and the tools to control them.

I. INTRODUCTION

In December 2010, the Federal Trade Commission ("FTC" or "Commission") issued a preliminary staff report to address the privacy issues associated with new technologies and business models.[1] The report outlined the FTC's 40-year history of promoting consumer privacy through policy and enforcement work, discussed the themes and areas of consensus that emerged from the Commission's "Exploring Privacy" roundtables, and set forth a proposed framework to guide policymakers and other stakeholders regarding best practices for consumer privacy. The proposed framework called on companies to build privacy protections into their business operations (*i.e.*, adopt "privacy by design"[2]), offer simplified choice mechanisms that give consumers more meaningful control, and increase the transparency of their data practices.

The preliminary report included a number of questions for public comment to assist and guide the Commission in developing a final privacy framework. The Commission received more than 450 comments from a wide variety of interested parties, including consumer and privacy advocates, individual companies and trade associations, academics, technologists, and domestic and foreign government agencies. Significantly, more than half of the comments came from individual consumers. The comments have helped the Commission refine the framework to better protect consumer privacy in today's dynamic and rapidly changing marketplace.

In this Final Report, the Commission adopts staff's preliminary framework with certain clarifications and revisions. The final privacy framework is intended to articulate best practices for companies that collect and use consumer data. These best practices can be useful to companies as they develop and maintain processes and systems to operationalize privacy and data security practices within their businesses. The final privacy framework contained in this Report is also intended to assist Congress as it considers privacy legislation. To the extent the framework goes beyond existing legal requirements, the framework is not intended to serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

The Report highlights the developments since the FTC issued staff's preliminary report, including the Department of Commerce's parallel privacy initiative, proposed legislation, and actions by industry and other stakeholders. Next, it analyzes and responds to the main issues raised by the public comments. Based on those comments, as well as marketplace developments, the Report sets forth a revised privacy framework and legislative recommendations. Finally, the Report outlines a series of policy initiatives that FTC staff will undertake in the next year to assist industry with implementing the final framework as best practices.

1 FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report* (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

2 Privacy by Design is an approach that Ann Cavoukian, Ph.D., Information and Privacy Commissioner, Ontario, Canada, has advocated. *See* Information and Privacy Commissioner, Ontario, Canada, Privacy by Design, http://privacybydesign.ca/.

II. BACKGROUND

A. FTC ROUNDTABLES AND PRELIMINARY STAFF REPORT

Between December 2009 and March 2010, the FTC convened its "Exploring Privacy" roundtables.[3] The roundtables brought together stakeholders representing diverse interests to evaluate whether the FTC's existing approach to protecting consumer privacy was adequate in light of 21st Century technologies and business models. From these discussions, as well as submitted materials, a number of themes emerged. First, the collection and commercial use of consumer data in today's society is ubiquitous and often invisible to consumers. Second, consumers generally lack full understanding of the nature and extent of this data collection and use and, therefore, are unable to make informed choices about it. Third, despite this lack of understanding, many consumers are concerned about the privacy of their personal information. Fourth, the collection and use of consumer data has led to significant benefits in the form of new products and services. Finally, the traditional distinction between personally identifiable information and "anonymous" data has blurred.

Participants also pointed to shortcomings in existing frameworks that have attempted to address privacy concerns. The "notice-and-choice model," which encouraged companies to develop privacy policies describing their information collection and use practices, led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand.[4] The "harm-based model," which focused on protecting consumers from specific harms – physical security, economic injury, and unwarranted intrusions into their daily lives – had been criticized for failing to recognize a wider range of privacy-related concerns, including reputational harm or the fear of being monitored.[5] Participants noted that both of these privacy frameworks have struggled to keep pace with the rapid growth of technologies and business models that enable companies to collect and use consumers' information in ways that often are invisible to consumers.[6]

Building on the record developed at the roundtables and on its own enforcement and policymaking expertise, FTC staff proposed for public comment a framework for approaching privacy. The proposed framework included three major components. It called on companies to treat privacy as their "default setting" by implementing "privacy by design" throughout their regular business operations. The concept of privacy by design includes limitations on data collection and retention, as well as reasonable security and data accuracy. By considering and addressing privacy at every stage of product and service development,

3 The first roundtable took place on December 7, 2009, the second roundtable on January 28, 2010, and the third roundtable on March 17, 2010. *See* FTC, *Exploring Privacy – A Roundtable Series*, http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

4 *See, e.g., 1st Roundtable, Remarks of Fred Cate, Indiana University Maurer School of Law*, at 280-81; *1st Roundtable, Remarks of Lorrie Cranor, Carnegie Mellon University*, at 129; *see also Written Comment of Fred Cate*, *2nd Roundtable, Consumer Protection in the Age of the 'Information Economy,'* cmt. #544506-00057, at 343-79.

5 *See, e.g., 1st Roundtable, Remarks of Marc Rotenberg, Electronic Privacy Information Center*, at 301; *1st Roundtable, Remarks of Leslie Harris, Center for Democracy & Technology*, at 36-38; *1st Roundtable, Remarks of Susan Grant, Consumer Federation of America*, at 38-39.

6 *See, e.g., 3rd Roundtable, Remarks of Kathryn Montgomery, American University School of Communication*, at 200-01; *2nd Roundtable, Remarks of Kevin Bankston, Electronic Frontier Foundation*, at 277.

companies can shift the burden away from consumers who would otherwise have to seek out privacy-protective practices and technologies. The proposed framework also called on companies to simplify consumer choice by presenting important choices – in a streamlined way – to consumers at the time they are making decisions about their data. As part of the call for simplified choice, staff asked industry to develop a mechanism that would allow consumers to more easily control the tracking of their online activities, often referred to as "Do Not Track." Finally, the framework focused on improving consumer understanding of commercial data practices ("transparency") and called on companies – both those that interact directly with consumers and those that lack a consumer interface – to improve the transparency of their practices. As discussed below, the Commission received a large number of thoughtful and informative comments regarding each of the framework's elements. These comments have allowed the Commission to refine the framework and to provide further guidance regarding its implementation.

B. DEPARTMENT OF COMMERCE PRIVACY INITIATIVES

In a related effort to examine privacy, in May 2010, the Department of Commerce ("DOC" or "Commerce") convened a public workshop to discuss how to balance innovation, commerce, and consumer privacy in the online context.[7] Based on the input received from the workshop, as well as related research, on December 16, 2010, the DOC published for comment a strategy paper outlining privacy recommendations and proposed initiatives.[8] Following the public comment period, on February 23, 2012, the Administration issued its final "White Paper" on consumer privacy. The White Paper recommends that Congress enact legislation to implement a Consumer Privacy Bill of Rights based on the Fair Information Practice Principles ("FIPPs").[9] In addition, the White Paper calls for a multistakeholder process to determine how to apply the Consumer Privacy Bill of Rights in different business contexts. Commerce issued a Notice of Inquiry on March 5, 2012, asking for public input on both the process for convening stakeholders on this project, as well as the proposed subject areas to be discussed.[10]

Staff from the FTC and Commerce worked closely to ensure that the agencies' privacy initiatives are complementary. Personnel from each agency actively participated in both the DOC and FTC initiatives, and have also communicated regularly on how best to develop a meaningful, effective, and consistent approach to privacy protection. Going forward, the agencies will continue to work collaboratively to guide implementation of these complementary privacy initiatives.

---

7 *See* Press Release, Department of Commerce, Commerce Secretary Gary Locke Discusses Privacy and Innovation with Leading Internet Stakeholders (May 7, 2010), *available at* http://www.commerce.gov/news/press-releases/2010/05/07/commerce-secretary-gary-locke-discusses-privacy-and-innovation-leadin.

8 *See* Department of Commerce Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Dec. 16, 2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf.

9 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The FIPPs as articulated in the Administration paper are: Transparency, Individual Control, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability.

10 *See* National Telecommunications and Information Administration, Request for Public Comment, Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 13098 (Mar. 5, 2012).

C. LEGISLATIVE PROPOSALS AND EFFORTS BY STAKEHOLDERS

Since Commission staff released its preliminary report in December 2010, there have been a number of significant legislative proposals, as well as steps by industry and other stakeholders, to promote consumer privacy.

1. DO NOT TRACK

The preliminary staff report called on industry to create and implement a mechanism to allow consumers to control the collection and use of their online browsing data, often referred to as "Do Not Track." Bills introduced in the House and the Senate specifically address the creation of Do Not Track mechanisms, and, if enacted, would mandate that the Commission promulgate regulations to establish standards for a Do Not Track regime.[11]

In addition to the legislative proposals calling for the creation of Do Not Track, staff's preliminary report recommendation triggered significant progress by various industry sectors to develop tools to allow consumers to control online tracking. A number of browser vendors – including Mozilla, Microsoft, and Apple – announced that the latest versions of their browsers permit consumers to instruct websites not to track their activities across websites.[12] Mozilla has also introduced a mobile browser for Android devices that enables Do Not Track.[13] The online advertising industry has also established an important program. The Digital Advertising Alliance ("DAA"), an industry coalition of media and marketing associations, has developed an initiative that includes an icon embedded in behaviorally targeted online ads.[14] When consumers click on the icon, they can see information about how the ad was targeted and delivered to them and they are given the opportunity to opt out of such targeted advertising. The program's recent growth and implementation has been significant. In addition, the DAA has committed to preventing the use of consumers' data for secondary purposes like credit and employment decisions. The DAA has also agreed to honor the choices about tracking that consumers make through settings on their web browsers. This will provide consumers two ways to opt out: through the DAA's icon in advertisements or through their browser settings. These steps demonstrate the online advertising industry's support for privacy and consumer choice.

---

11 *See* Do-Not-Track Online Act of 2011, S. 913, 112th Congress (2011); Do Not Track Me Online Act, H.R. 654, 112th Congress (2011).

12 *See* Press Release, Microsoft, Providing Windows Customers with More Choice and Control of Their Privacy Online with Internet Explorer 9 (Dec. 7, 2010), *available at* http://www.microsoft.com/presspass/features/2010/dec10/12-07ie9privacyqa.mspx; *Mozilla Firefox 4 Beta, Now Including "Do Not Track" Capabilities*, Mozilla Blog (Feb. 8, 2011), http://blog.mozilla.com/blog/2011/02/08/mozilla-firefox-4-beta-now-including-do-not-track-capabilities/; Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, Wall St. J., Apr. 13, 2011, *available at* http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html. Google recently announced that it will also offer this capability in the next version of its browser. Gregg Kaizer, *FAQ: What Google's Do Not Track Move Means*, Computerworld (Feb. 24, 2012), *available at* http://www.computerworld.com/s/article/9224583/FAQ_What_Google_s_Do_Not_Track_move_means.

13 *See* Mozilla, Do Not Track FAQs, http://dnt.mozilla.org.

14 *See* Press Release, Interactive Advertising Bureau, Major Marketing/Media Trade Groups Launch Program to Give Consumers Enhanced Control Over Collection and Use of Web Viewing Data for Online Behavioral Advertising (Oct. 4, 2010), *available at* http://www.iab.net/about_the_iab/recent_press_releases/press_release_archive/press_release/pr-100410.

Finally, the World Wide Web Consortium ("W3C")[15] convened a working group to create a universal standard for Do Not Track. The working group includes DAA member companies, other U.S. and international companies, industry groups, and consumer groups. The W3C group has made substantial progress toward a standard that is workable in the desktop and mobile settings, and has published two working drafts of its standard documents. The group's goal is to complete a consensus standard in the coming months.

2. OTHER PRIVACY INITIATIVES

Beyond the Do Not Track developments, broader initiatives to improve consumer privacy are underway in Congress, Federal agencies, and the private sector. For example, Congress is considering several general privacy bills that would establish a regulatory framework for protecting consumer privacy by improving transparency about the commercial uses of personal information and providing consumers with choice about such use.[16] The bills would also provide the Commission rulemaking authority concerning, among other things, notice, consent, and the transfer of information to third parties.

In the House of Representatives, Members have introduced bipartisan legislation to amend the Children's Online Privacy Protection Act[17] ("COPPA") and establish other protections for children and teens.[18] The bill would prohibit the collection and use of minors' information for targeted marketing and would require websites to permit the deletion of publicly available information of minors. Members of Congress also introduced a number of other bills addressing data security and data breach notification in 2011.[19]

15 The W3C is an international standard-setting body that works "to lead the World Wide Web to its full potential by developing protocols and guidelines that ensure the long-term growth of the Web." *See* W3C Mission, http://www.w3.org/Consortium/mission.html.

16 *See* Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Congress (2011); Building Effective Strategies To Promote Responsibility Accountability Choice Transparency Innovation Consumer Expectations and Safeguards Act, H.R. 611, 112th Congress (2011); Consumer Privacy Protection Act of 2011, H.R. 1528, 112th Congress (2011).

17 Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506.

18 *See* Do Not Track Kids Act of 2011, H.R. 1895, 112th Congress (2011). In September 2011, the Commission issued a Notice of Proposed Rulemaking, proposing changes to the COPPA Rule to address changes in technology. *See FTC Children's Online Privacy Protection Rule*, 76 Fed. Reg. 59804 (proposed Sep. 27, 2011), *available at* http://www.ftc.gov/os/2011/09/110915coppa.pdf.

19 *See* Personal Data Privacy and Security Act of 2011, S. 1151, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011); Data Breach Notification Act of 2011, S.1408, 112th Congress (2011); Data Security Act of 2011, S.1434, 112th Congress (2011); Personal Data Protection and Breach Accountability Act of 2011, S. 1535, 112th Congress (2011); Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Secure and Fortify Electronic Data Act, H.R. 2577, 112th Congress (2011).

Federal agencies have taken significant steps to improve consumer privacy as well. For its part, since issuing the preliminary staff report, the FTC has resolved seven data security cases,[20] obtained orders against Google, Facebook, and online ad networks,[21] and challenged practices that violate sector-specific privacy laws like the Fair Credit Reporting Act ("FCRA") and COPPA.[22] The Commission has also proposed amendments to the COPPA Rule to address changes in technology. The comment period on the Proposed Rulemaking ran through December 23, 2011, and the Commission is currently reviewing the comments received.[23] Additionally, the Commission has hosted public workshops on discrete privacy issues such as child identity theft and the use of facial recognition technology.

Other federal agencies have also begun examining privacy issues. In 2011, the Federal Communications Commission ("FCC") hosted a public forum to address privacy concerns associated with location-based services.[24] The Department of Health and Human Services ("HHS") hosted a forum on medical identity theft, developed a model privacy notice for personal health records,[25] and is developing legislative recommendations on privacy and security for such personal health records. In addition, HHS recently launched an initiative to identify privacy and security best practices for using mobile devices in health care settings.[26]

---

20 *See In the Matter of Upromise, Inc.,* FTC File No. 102 3116 (Jan. 18, 2012) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/1023116/index.shtm; *In the Matter of ACRAnet, Inc.*, FTC Docket No. C-4331 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923088/index.shtm; *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0823208/index.shtm; *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023160/index.shtm; *In the Matter of Lookout Servs., Inc.,* FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023076/index.shtm; *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923093/index.shtm; *In the Matter of Fajilan & Assocs., Inc.,* FTC Docket No. C-4332 (Aug. 17, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923089/index.shtm.

21 *See In the Matter of Google, Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023136/index.shtm (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/index.shtm (requiring company to implement privacy program subject to independent third-party audit); *In the Matter of Chitika, Inc.*, FTC Docket No. C-4324 (June 7, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023087/index.shtm (requiring company's behavioral advertising opt out to last for five years); *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 14, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023185/index.shtm (requiring company to improve disclosure of its data collection practices and offer consumers a user-friendly opt out mechanism).

22 Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*; COPPA Rule, 16 C.F.R. Part 312; *see also, e.g.*, *United States v. W3 Innovations, LLC*, No. CV-11-03958 (N.D. Cal. Sept. 8, 2011) (COPPA consent decree); *United States v. Teletrack, Inc.*, No. 1 11-CV-2060 (N.D. Ga. filed June 24, 2011) (FCRA consent decree); *United States v. Playdom, Inc.*, No. SACV-11-00724-AG (ANx) (C.D. Cal. May 24, 2011) (COPPA consent decree).

23 *See* Press Release, FTC Extends Deadline for Comments on Proposed Amendments to the Children's Online Privacy Protection Rule Until December 23 (Nov. 18, 2011), *available at* http://www.ftc.gov/opa/2011/11/coppa.shtm.

24 *See* FCC Workshop, *Helping Consumers Harness the Potential of Location-Based Services* (June 28, 2011), *available at* http://www.fcc.gov/events/location-based-services-forum.

25 *See* The Office of the National Coordinator for Health Information Technology, Personal Health Record (PHR) Model Privacy Notice, http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__draft_phr_model_notice/1176.

26 *See* HHS Workshop, *Mobile Devices Roundtable: Safeguarding Health Information*, *available at* http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__mobile_devices_roundtable/3815.

The private sector has taken steps to enhance user privacy and security as well. For example, Google and Facebook have improved authentication mechanisms to give users stronger protection against compromised passwords.[27] Also, privacy-enhancing technologies such as the HTTPS Everywhere browser add-on have given users additional tools to encrypt their information in transit.[28] On the mobile front, the Mobile Marketing Association released its Mobile Application Privacy Policy.[29] This document provides guidance on privacy principles for application ("app") developers and discusses how to inform consumers about the collection and use of their data. Despite these developments, as explained below, industry still has more work to do to promote consumer privacy.

III. MAIN THEMES FROM COMMENTERS

The more than 450 comments filed in response to the preliminary staff report addressed three overarching issues: how privacy harms should be articulated; the value of global interoperability of different privacy regimes; and the desirability of baseline privacy legislation to augment self-regulatory efforts. Those comments, and the Commission's analysis, are discussed below.

A. ARTICULATION OF PRIVACY HARMS

There was broad consensus among commenters that consumers need basic privacy protections for their personal information. This is true particularly in light of the complexity of the current personal data ecosystem. Some commenters also stated that the Commission should recognize a broader set of privacy harms than those involving physical and economic injury.[30] For example, one commenter cited complaints from consumers who had been surreptitiously tracked and targeted with prescription drug offers and other health-related materials regarding sensitive medical conditions.[31]

At the same time, some commenters questioned whether the costs of broader privacy protections were justified by the anticipated benefits.[32] Relatedly, many commenters raised concerns about how wider privacy protections would affect innovation and the ability to offer consumers beneficial new products and services.[33]

---

27 *See Advanced Sign-In Security For Your Google Account*, Google Official Blog (Feb. 10, 2011, 11:30 AM), http://googleblog.blogspot.com/2011/02/advanced-sign-in-security-for-your.html#!/2011/02/advanced-sign-in-security-for-your.html; Andrew Song, *Introducing Login Approvals*, Facebook Blog (May 12, 2011, 9:58 AM), http://www.facebook.com/note.php?note_id=10150172618258920.

28 *See HTTPS Everywhere*, Electronic Frontier Foundation, https://www.eff.org/https-everywhere.

29 *See* Press Release, Mobile Marketing Association, Mobile Marketing Association Releases Final Privacy Policy Guidelines for Mobile Apps (Jan. 25, 2012), *available at* http://mmaglobal.com/news/mobile-marketing-association -releases-final-privacy-policy-guidelines-mobile-apps.

30 *See Comment of TRUSTe*, cmt. #00450, at 3; *Comment of Berlin Commissioner for Data Protection & Freedom of Information*, cmt. #00484, at 1.

31 *See Comment of Patient Privacy Rights*, cmt. #00470, at 2.

32 *See Comment of Technology Policy Institute*, cmt. #00301, at 5-8; *Comment of Experian*, cmt. #00398, at 9-11; *Comment of Global Privacy Alliance*, cmt. #00367, at 6-7.

33 *See Comment of Facebook, Inc.,* cmt. #00413, at 1-2, 7-8; *Comment of Google, Inc.*, cmt. #00417, at 4; *Comment of Global Privacy Alliance*, cmt. #00367, at 16.

The Commission agrees that the range of privacy-related harms is more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data. These harms may include the unexpected revelation of previously private information, including both sensitive information (*e.g.*, health information, precise geolocation information) and less sensitive information (*e.g.*, purchase history, employment history) to unauthorized third parties.[34] As one example, in the Commission's case against Google, the complaint alleged that Google used the information of consumers who signed up for Gmail to populate a new social network, Google Buzz.[35] The creation of that social network in some cases revealed previously private information about Gmail users' most frequent email contacts. Similarly, the Commission's complaint against Facebook alleged that Facebook's sharing of users' personal information beyond their privacy settings was harmful.[36] Like these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions.[37]

In terms of weighing costs and benefits, although it recognizes that imposing new privacy protections will not be costless, the Commission believes doing so not only will help consumers but also will benefit businesses by building consumer trust in the marketplace. Businesses frequently acknowledge the importance of consumer trust to the growth of digital commerce[38] and surveys support this view. For

34 One former FTC Chairman, in analyzing a spyware case, emphasized that consumers should have control over what is on their computers. Chairman Majoras issued the following statement in connection with the Commission's settlement against Sony BMG resolving claims about the company's installation of invasive tracking software: "Consumers' computers belong to them, and companies must adequately disclose unexpected limitations on the customary use of their products so consumers can make informed decisions regarding whether to purchase and install that content." Press Release, FTC, Sony BMG Settles FTC Charges (Jan. 30, 2007), *available at* http://www.ftc.gov/opa/2007/01/sony.shtm; *see also* Walt Mossberg, *Despite Others' Claims, Tracking Cookies Fit My Spyware Definition*, AllThingsD (July 14, 2005, 12:01 AM), http://allthingsd.com/20050714/tracking-cookies/ ("Suppose you bought a TV set that included a component to track what you watched, and then reported that data back to a company that used or sold it for advertising purposes. Only nobody told you the tracking technology was there or asked your permission to use it. You would likely be outraged at this violation of privacy. Yet that kind of Big Brother intrusion goes on everyday on the Internet . . . [with tracking cookies].").

35 *See In re Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcompt.pdf.

36 *See In re Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

37 Although the complaint against Google alleged that the company used deceptive tactics and violated its own privacy promises when it launched Google Buzz, even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm. *See* Press Release, FTC, FTC Charges Deceptive Privacy Practices in Google's Rollout of its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm (noting that in response to the Buzz launch, Google received thousands of complaints from consumers who were concerned about public disclosure of their email contacts which included, in some cases, ex-spouses, patients, students, employers, or competitors).

38 *See, e.g.*, Statement of John M. Montgomery, GroupM Interaction, *The State of Online Consumer Privacy*: *Hearing Before the S. Comm. on Commerce, Sci., and Transp.*, 112th Cong. (Mar. 16, 2011), *available at* http://www.iab.net/media/file/DC1DOCS1-432016-v1-John_Montgomery_-_Written_Testimony.pdf ("We at GroupM strongly believe in protecting consumer privacy. It is not only the right thing to do, but it is also good for business."); Statement of Alan Davidson, Director of Public Policy, Google Inc., *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy: Hearing Before the S. Subcomm. on Privacy, Tech., and the Law*, 112th Cong. (May 10, 2011), *available at* http://www.judiciary.senate.gov/pdf/11-5-10%20Davidson%20Testimony.pdf ("Protecting privacy and security is essential for Internet commerce.").

example, in the online behavioral advertising area, a recent survey shows that consumers feel better about brands that give them transparency and control over advertisements.[39]

Companies offering consumers information about behavioral advertising and the tools to opt out of it have also found increased customer engagement. In its comment, Google noted that visitors to its Ads Preference Manager are far more likely to edit their interest settings and remain opted in rather than to opt out.[40] Similarly, another commenter conducted a study showing that making its customers aware of its privacy and data security principles – including restricting the sharing of customer data, increasing the transparency of data practices, and providing access to the consumer data it maintains – significantly increased customer trust in its company.[41]

In addition, some companies appear to be competing on privacy. For example, one company offers an Internet search service that it promotes as being far more privacy-sensitive than other search engines.[42] Similarly, in response to Google's decision to change its privacy policies to allow tracking of consumers across different Google products, Microsoft encouraged consumers to switch to Microsoft's more privacy-protective products and services.[43]

The privacy framework is designed to be flexible to permit and encourage innovation. Companies can implement the privacy protections of the framework in a way that is proportional to the nature, sensitivity, and amount of data collected as well as to the size of the business at issue. For example, the framework does not include rigid provisions such as specific disclosures or mandatory data retention and destruction periods. And, as discussed below, the framework streamlines communications for businesses and consumers alike by requiring consumer choice mechanisms only for data practices that are inconsistent with the context of a particular transaction or the business relationship with the consumer.[44]

B. GLOBAL INTEROPERABILITY

Reflecting differing legal, policy, and constitutional regimes, privacy frameworks around the world vary considerably. Many commenters cited the value to both consumers and businesses of promoting more consistent and interoperable approaches to protecting consumer privacy internationally. These commenters stated that consistency between different privacy regimes reduces companies' costs, promotes international competitiveness, and increases compliance with privacy standards.[45]

---

39 *See RESEARCH: Consumers Feel Better About Brands That Give Them Transparency and Control Over Ads*, Evidon Blog (Nov. 10, 2010), http://blog.evidon.com/tag/better-advertising ("when advertisers empower consumers with information and control over the ads they receive, a majority feels more positive toward those brands, and 36% even become more likely to purchase from those brands").

40 *See Comment of Google Inc.*, cmt. #00417, at 4.

41 *See Comment of Intuit, Inc.*, cmt. #00348, at 6-8 ("The more transparent (meaning open, simple and clear) the company is, the more customer trust increases. . . .").

42 *See* DuckDuckGo, Privacy Policy, https://duckduckgo.com/privacy.html.

43 *See* Frank X. Shaw, *Gone Google? Got Concerns? We Have Alternatives*, The Official Microsoft Blog (Feb. 1, 2012, 2:00 AM), http://blogs.technet.com/b/microsoft_blog/archive/2012/02/01/gone-google-got-concerns-we-have-alternatives.aspx.

44 See *infra* at Section IV.C.1.a.

45 *See Comment of AT&T Inc.*, cmt. #00420, at 12-13; *Comment of IBM*, cmt. #00433, at 2; *see also Comment of General Electric*, cmt. #00392, at 3 (encouraging international harmonization).

The Commission agrees there is value in greater interoperability among data privacy regimes as consumer data is increasingly transferred around the world. Meaningful protection for such data requires convergence on core principles, an ability of legal regimes to work together, and enhanced cross-border enforcement cooperation. Such interoperability is better for consumers, whose data will be subject to more consistent protection wherever it travels, and more efficient for businesses by reducing the burdens of compliance with differing, and sometimes conflicting, rules. In short, as the Administration White Paper notes, global interoperability "will provide more consistent protections for consumers and lower compliance burdens for companies."[46]

Efforts underway around the world to re-examine current approaches to protecting consumer privacy indicate an interest in convergence on overarching principles and a desire to develop greater interoperability. For example, the Commission's privacy framework is consistent with the nine privacy principles set forth in the 2004 Asia-Pacific Economic Cooperation ("APEC") Privacy Framework. Those principles form the basis for ongoing APEC work to implement a cross-border privacy rules system to facilitate data transfers among the 21 APEC member economies, including the United States.[47] In 2011, the Organization for Economic Cooperation and Development ("OECD") issued a report re-examining its seminal 1980 Privacy Guidelines in light of technological changes over the past thirty years.[48] Further, the European Commission has recently proposed legislation updating its 1995 data protection directive and proposed an overhaul of the European Union approach that focuses on many of the issues raised elsewhere in this report as well as issues relating to international transfers and interoperability.[49] These efforts reflect a commitment to many of the high-level principles embodied in the FTC's framework – increased transparency and consumer control, the need for privacy protections to be built into basic business practices, and the importance of accountability and enforcement. They also reflect a shared international interest in having systems that work better with each other, and are thus better for consumers.

46 White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, ii, Foreword (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

47 The nine principles in the APEC Privacy Framework are preventing harm, notice, collection limitations, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, accountability. Businesses have developed a code of conduct based on these nine principles and will obtain third-party certification of their compliance. A network of privacy enforcement authorities from participating APEC economies, such as the FTC, will be able to take enforcement actions against companies that violate their commitments under the code of conduct. *See* Press Release, FTC, FTC Welcomes a New Privacy System for the Movement of Consumer Data Between the United States and Other Economies in the Asia-Pacific Region (Nov. 14, 2011), *available at* http://www.ftc.gov/opa/2011/11/apec.shtm).

48 *See* Organization for Economic Co-operation and Development, *The Evolving Privacy Landscape: 30 Years after the OECD Privacy Guidelines* (Apr. 2011), *available at* http://www.oecd.org/dataoecd/22/25/47683378.pdf.

49 European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

C. LEGISLATION TO AUGMENT SELF-REGULATORY EFFORTS

Numerous comments, including those from large industry stakeholders, consumer and privacy advocates, and individual consumers supported some form of baseline privacy legislation that incorporates the FIPPs.[50] Business commenters noted that legislation would help provide legal certainty,[51] serve as a key mechanism for building trust among customers,[52] and provide a way to fill gaps in existing sector-based laws.[53] Consumer and privacy advocates cited the inability of self-regulation to provide comprehensive and long-lasting protection for consumers.[54] One such commenter cited the fact that many self-regulatory initiatives that arose in response to the Commission's 2000 recommendation for privacy legislation were short-lived and failed to provide long-term privacy protections for consumers.[55]

At the same time, a number of commenters raised concerns about government action beyond providing guidance for self-regulatory programs.[56] Some cautioned the FTC about taking an approach that might impede industry's ability to innovate and develop new products and services in a rapidly changing marketplace. Others noted that a regulatory approach could lead to picking "winners and losers" among particular technologies and business models and called for a technology-neutral approach.[57] Commenters also argued that it might be impractical to craft omnibus standards or rules that would apply broadly across different business sectors.[58]

The Commission agrees that, to date, self-regulation has not gone far enough. In most areas, with the notable exception of efforts surrounding Do Not Track, there has been little self-regulation. For example, the FTC's recent survey of mobile apps marketed to children revealed that many of these apps fail to provide any disclosure about the extent to which they collect and share consumers' personal data.[59] Similarly, efforts

50 *See, e.g.*, *Comment of eBay*, cmt. #00374, at 2; *Comment of Intel Corp.*, cmt. #00246, at 3-7; *Comment of Microsoft Corp.*, cmt. #00395, at 4; *Comment of Intuit, Inc.*, cmt. #00348, at 13-14; *Comment of Center for Democracy & Technology*, cmt. #00469, at 1, 7; *Comment of Gregory Byrd*, cmt. #00144, at 1; *Comment of Ellen Klinefelter*, cmt. #00095, at 1.

51 *See Comment of Microsoft Corp.*, cmt. #00395, at 4.

52 *See Comment of Intel Corp.*, cmt. #00246, at 3.

53 *See Comment of Intuit, Inc.*, cmt. #00348, at 13.

54 *See Comment of Electronic Privacy Information Center*, cmt. #00386, at 2; *Comment of World Privacy Forum*, cmt. #00376, at 2-3, 8-17.

55 *See Comment of World Privacy Forum*, cmt. #00376, at 2-3, 8-17.

56 *See Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4-5; *Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 3; *Comment of Facebook, Inc.*, cmt. #00413, at 13-14; *Comment of Google Inc.*, cmt. #00417, at 8; *Comment of Verizon*, cmt. #00428, at 2-3, 6-7, 14-17; *Comment of Mortgage Bankers Ass'n*, cmt. #00308, at 2; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 3, 5, 7-13; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 15.

57 *See Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 32-37; *Comment of USTelecom*, cmt. #00411, at 5-7; *Comment of Verizon*, cmt. #00428, at 4-6; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 5-6.

58 *See Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4-6; *see also Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 8-11; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 13.

59 FTC Staff, *Mobile Apps for Kids: Current Privacy Disclosures are Disappointing* (Feb. 2012), *available at* http://www.ftc.gov/os/2012/02/120216mobile_apps_kids.pdf; *FPF Finds Nearly Three-Quarters of Most Downloaded Mobile Apps Lack a Privacy Policy*, Future of Privacy Forum, http://www.futureofprivacy.org/2011/05/12/fpf-finds-nearly-three-quarters-of-most-downloaded-mobile-apps-lack-a-privacy-policy/.

of the data broker industry to establish self-regulatory rules concerning consumer privacy have fallen short.[60] These examples illustrate that even in some well-established markets, basic privacy concepts like transparency about the nature of companies' data practices and meaningful consumer control are absent. This absence erodes consumer trust.

There is also widespread evidence of data breaches and vulnerabilities related to consumer information.[61] Published reports indicate that some breaches may have resulted from the unintentional release of consumer data, for which companies later apologized and took action to address.[62] Other incidents involved planned releases or uses of data by companies that ultimately did not occur due to consumer and public backlash.[63] Still other incidents involved companies' failure to take reasonable precautions and resulted in FTC consent decrees. These incidents further undermine consumer trust, which is essential for business growth and innovation.[64]

The ongoing and widespread incidents of unauthorized or improper use and sharing of personal information are evidence of two points. First, companies that do not intend to undermine consumer privacy simply lack sufficiently clear standards to operate and innovate while respecting the expectations of consumers. Second, companies that do seek to cut corners on consumer privacy do not have adequate legal incentives to curtail such behavior.

To provide clear standards and appropriate incentives to ensure basic privacy protections across all industry sectors, in addition to reiterating its call for federal data security legislation,[65] the Commission calls

60 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 2-3; *Comment of World Privacy Forum*, cmt. #00376, at 2-3. Discussed more fully *infra* at Section IV.D.2.a.

61 *See* Grant Gross, *Lawmakers Question Sony, Epsilon on Data Breaches,* PC World (June 2, 2011 3:40 PM), *available at* http://www.pcworld.com/businesscenter/article/229258/lawmakers_question_sony_epsilon_on_data_breaches.html; Dwight Silverman, *App Privacy: Who's Uploading Your Contact List?*, Houston Chronicle (Feb. 15, 2012 8:10 AM), http://blog.chron.com/techblog/2012/02/app-privacy-whos-uploading-your-contact-list/; Dan Graziano, *Like iOS apps, Android Apps Can Secretly Access Photos Thanks to Loophole,* BGR (Mar. 1, 2012 3:45 PM), http://www.bgr.com/2012/03/01/like-ios-apps-android-apps-can-also-secretly-access-photos-thanks-to-security-hole/.

62 *CEO Apologizes After Path Social App Uploads Contact Lists,* KMOV.com (Feb. 9, 2012 11:11AM), http://www.kmov.com/news/consumer/CEO-apologizes-after-Path-uploads-contact-lists--139015729.html; Daisuke Wakabayashi, *A Contrite Sony Vows Tighter Security,* Wall St. J. May 1, 2011, *available at* http://online.wsj.com/article/SB10001424052748704436004576296302384608280.html.

63 Kevin Parrish, *OnStar Changes its Mind About Tracking Vehicles,* Tom's Guide (Sept. 29, 2011 7:30 AM), http://www.tomsguide.com/us/OnStar-General-motors-Linda-Marshall-GPS-Terms-and-conditions,news-12677.html.

64 Surveys of consumer attitudes towards privacy conducted in the past year are illuminating. For example, a *USA Today*/Gallup poll indicated that a majority of the Facebook members or Google users surveyed were "very" or "somewhat concerned" about their privacy while using these services. Lymari Morales, *Google and Facebook Users Skew Young, Affluent, and Educated*, Gallup (Feb. 17, 2011), *available at* http://www.gallup.com/poll/146159/facebook-google-users-skew-young-affluent-educated.aspx.

65 The Commission has long supported federal laws requiring companies to implement reasonable security measures and to notify consumers in the event of certain security breaches. *See, e.g.*, Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC, *Protecting Social Security Numbers From Identity Theft*: *Hearing Before the Before the H. Comm. on Ways and Means, Subcomm. on Social Security*, 112th Cong. (April 13, 2011), *available at* http://www.ftc.gov/os/testimony/110411ssn-idtheft.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), *available at* http://www.ftc.gov/os/2008/12/P075414ssnreport.pdf; President's Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), *available at* http://www.idtheft.gov/reports/IDTReport2008.pdf.

on Congress to consider enacting baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate. The Commission is prepared to work with Congress and other stakeholders to craft such legislation.

In their comments, many businesses indicated that they already incorporate the FIPPS into their practices. For these companies, a legislative mandate should not impose an undue burden and indeed, will "level the playing field" by ensuring that all companies are required to incorporate these principles into their practices.

For those companies that are not already taking consumer privacy into account – either because of lack of understanding or lack of concern – legislation should provide clear rules of the road. It should also provide adequate deterrence through the availability of civil penalties and other remedies.[66] In short, legislation will provide businesses with the certainty they need to understand their obligations and the incentive to meet those obligations, while providing consumers with confidence that businesses will be required to respect their privacy. This approach will create an environment that allows businesses to continue to innovate and consumers to embrace those innovations without sacrificing their privacy.[67] The Commission is prepared to work with Congress and other stakeholders to formulate baseline privacy legislation.

While Congress considers such legislation, the Commission urges industry to accelerate the pace of its self-regulatory measures to implement the Commission's final privacy framework. Over the course of the next year, Commission staff will promote the framework's implementation by focusing its policymaking efforts on five main action items, which are highlighted here and discussed further throughout the report.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.
- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures.[68] As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to

66 Former FTC Chairman Casper "Cap" Weinberger recognized the value of civil penalties as a deterrent to unlawful conduct. *See Hearings on H.R. 14931 and Related Bills before the Subcomm. on Commerce and Finance of the H. Comm. on Interstate and Foreign Commerce*, 91st Cong. 53, 54 (1970) (statement of FTC Chairman Caspar Weinberger); *Hearings on S. 2246, S. 3092, and S. 3201 Before the Consumer Subcomm. of the S. Comm. on Commerce*, 91st Cong. 9 (1970) (Letter from FTC Chairman Caspar W. Weinberger) (forwarding copy of House testimony).

67 With this report, the Commission is not seeking to impose civil penalties for privacy violations under the FTC Act. Rather, in the event Congress enacts privacy legislation, the Commission believes that such legislation would be more effective if the FTC were authorized to obtain civil penalties for violations.

68 *See* Press Release, FTC, FTC Seeks Input to Revising its Guidance to Businesses About Disclosures in Online Advertising (May 26, 2011), *available at* http://www.ftc.gov/opa/2011/05/dotcom.shtm.

consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.

- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker.[69] To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers ("ISPs"), operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.
- **Promoting enforceable self-regulatory codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

69 *See* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).

IV. PRIVACY FRAMEWORK

In addition to the general comments described above, the Commission received significant comments on the scope of the proposed framework and each individual element. Those comments, as well as several clarifications and refinements based on the Commission's analysis of the issues raised, are discussed below.

A. SCOPE

Proposed Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device.

A variety of commenters addressed the framework's proposed scope. Some of these commenters supported an expansive reach while others proposed limiting the framework's application to particular types of entities and carving out certain categories of businesses. Commenters also called for further clarification regarding the type of data the framework covers and staff's proposed "reasonably linked" standard.

1. COMPANIES SHOULD COMPLY WITH THE FRAMEWORK UNLESS THEY HANDLE ONLY LIMITED AMOUNTS OF NON-SENSITIVE DATA THAT IS NOT SHARED WITH THIRD PARTIES.

Numerous commenters addressed whether the framework should apply to entities that collect, maintain, or use limited amounts of data. Several companies argued that the burden the framework could impose on small businesses outweighed the reduced risk of harm from the collection and use of limited amounts of non-sensitive consumer data.[70] These commenters proposed that the framework not apply to entities that collect or use non-sensitive data from fewer than 5,000 individuals a year where the data is used for limited purposes, such as internal operations and first-party marketing.[71] As additional support for this position, these commenters noted that proposed privacy legislation introduced in the 111th Congress contained an exclusion to this effect.[72]

Although one consumer and privacy organization supported a similar exclusion,[73] others expressed concern about exempting, *per se*, any types of businesses or quantities of data from the framework's scope.[74] These commenters pointed to the possibility that excluded companies would sell the data to third parties, such as advertising networks or data brokers.

The Commission agrees that the first-party collection and use of non-sensitive data (*e.g.*, data that is not a Social Security number or financial, health, children's, or geolocation information) creates fewer privacy

70 *See Comment of eBay, Inc.*, cmt. #00374, at 3; *Comment of Microsoft Corp.*, cmt. #00395, at 4.

71 *Id.*

72 *See* BEST PRACTICES ACT, H.R. 5777, 111th Congress (2010); Staff Discussion Draft, H.R. __ , 111th Congress (2010), *available at* http://www.nciss.org/legislation/BoucherStearnsprivacydiscussiondraft.pdf.

73 *Comment of the Center for Democracy & Technology*, cmt. #00469, at 1.

74 *See Comment of the Electronic Frontier Foundation*, cmt. #00400, at 1; *Comment of the Consumer Federation of America*, cmt. #00358, at 2.

concerns than practices that involve sensitive data or sharing with third parties.[75] Accordingly, entities that collect limited amounts of non-sensitive consumer data from under 5,000 consumers need not comply with the framework, as long as they do not share the data with third parties. For example, consider a cash-only curb-side food truck business that offers to send messages announcing when it is in a given neighborhood to consumers who provide their email addresses. As long as the food truck business does not share these email addresses with third parties, the Commission believes that it need not provide privacy disclosures to its customers. This narrow exclusion acknowledges the need for flexibility for businesses that collect limited amounts of non-sensitive information. It also recognizes that some business practices create fewer potential risks to consumer information.

2. THE FRAMEWORK SETS FORTH BEST PRACTICES AND CAN WORK IN TANDEM WITH EXISTING PRIVACY AND SECURITY STATUTES.

The proposed framework's applicability to commercial sectors that are covered by existing laws generated comments primarily from representatives of the healthcare and financial services industries. These commenters noted that statutes such as the Health Insurance Portability and Accountability Act ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and the Gramm-Leach-Bliley Act ("GLBA") already impose privacy protections and security requirements through legal obligations on companies in these industries.[76] Accordingly, these commenters urged the Commission to avoid creating duplicative or inconsistent standards and to clarify that the proposed framework is intended to cover only those entities that are not currently covered by existing privacy and security laws. Another commenter, however, urged government to focus on fulfilling consumer privacy expectations across all sectors, noting that market evolution is blurring distinctions about who is covered by HIPAA and that consumers expect organizations to protect their personal health information, regardless of any sector-specific boundaries.[77]

The Commission recognizes the concern regarding potentially inconsistent privacy obligations and notes that, to the extent Congress enacts any of the Commission's recommendations through legislation, such legislation should not impose overlapping or duplicative requirements on conduct that is already regulated.[78] However, the framework is meant to encourage best practices and is not intended to conflict with requirements of existing laws and regulations. To the extent that components of the framework exceed, but do not conflict with existing statutory requirements, entities covered by those statutes should view the framework as best practices to promote consumer privacy. For example, it may be appropriate for financial institutions covered by GLBA to incorporate elements of privacy by design, such as collection limitations, or

75 See *infra* at Sections IV.C.1.b.(v) and IV.C.2.e.(ii), for a discussion of what constitutes sensitive data.

76 *See Comment of the Confidentiality Coalition c/o the Healthcare Leadership Council*, cmt. #00349, at 1-4; *Comment of Experian*, cmt. #00398, at 8-10; *Comment of IMS Health*, cmt. #00380, at 2-3; *Comment of Medco Health Solutions, Inc.*, cmt. #00393, at 3; *Comment of SIFMA*, cmt. #00265, at 2-3.

77 *Comment of The Markle Foundation*, cmt. #00456, at 3-10.

78 Any baseline privacy law Congress may enact would likely consider the best way to take into account obligations under existing statutes.

to improve transparency by providing reasonable access to consumer data in a manner that does not conflict with their statutory obligations. In any event, the framework provides an important baseline for entities that are not subject to sector-specific laws like HIPAA or GLBA.[79]

3. THE FRAMEWORK APPLIES TO OFFLINE AS WELL AS ONLINE DATA.

In addressing the framework's applicability to "all commercial entities," numerous commenters discussed whether the framework should apply to both online and offline data. Diverse commenters expressed strong support for a comprehensive approach applicable to both online and offline data practices.[80] Commenters noted that as a practical matter, many companies collect both online and offline data.[81]

Commenters also listed different offline contexts in which entities collect consumer data. These include instances where a consumer interacts directly with a business, such as through the use of a retail loyalty card, or where a non-consumer facing entity, such as a data broker, obtains consumer data from an offline third-party source.[82] One commenter noted that, regardless of whether an entity collects or uses data from an online or an offline source, consumer privacy interests are equally affected.[83] To emphasize the importance of offline data protections, this commenter noted that while the behavioral advertising industry has started to implement self-regulatory measures to improve consumers' ability to control the collection and the use of their online data, in the offline context such efforts by data brokers and others have largely failed.[84]

By contrast, a financial industry organization argued that the FTC should take a more narrow approach by limiting the scope of the proposed framework in a number of respects, including its applicability to offline data collection and use.[85] This commenter stated that some harms in the online context may not exist offline and raised concern about the framework's unintended consequences. For example, the commenter cited the significant costs that a requirement to provide consumers with access to data collected about them

79 There may be entities that operate within covered sectors but that nevertheless fall outside of a specific law's scope. For instance, a number of entities that collect health information are not subject to HIPAA. These entities include providers of personal health records – online portfolios that consumers can use to store and keep track of their medical information. In 2009, Congress passed the HITECH Act, which required HHS, in consultation with the FTC, to develop legislative recommendations on privacy and security requirements that should apply to these providers of personal health records and related entities. Health Information Technology ("HITECH") Provisions of American Recovery and Reinvestment Act of 2009, Title XIII, Subtitle D (Pub. L. 111-5, 123 Stat. 115, codified in relevant part at 42 U.S.C. §§ 17937 and 17954). FTC staff is consulting with HHS on this project.

80 *See Comment of the Center for Democracy & Technology,* cmt. #00469, at 2; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14; *Comment of Consumers Union*, cmt. #00362, at 4-5; *Comment of the Department of Veterans Affairs*, cmt. #00479, at 3; *Comment of Experian*, cmt. #00398, at 1; *Comment of Google Inc.*, cmt. #00417, at 7; *Comment of Microsoft Corp.*, cmt. #00395, at 4.

81 *See Comment of the Department of Veterans Affairs*, cmt. #00479, at 3 n.7; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14; *Comment of Consumers Union*, cmt. #00362, at 1.

82 *See Comment of the Department of Veterans Affairs*, cmt. #00479, at 3 n.7; *Comment of the Computer & Communications Industry Ass'n*, cmt. #00434, at 14.

83 *Comment of Center for Democracy & Technology*, cmt. #00469, at 2.

84 *Comment of Center for Democracy & Technology*, cmt. #00469, at 2-3.

85 *Comment of the Financial Services Forum*, cmt. #00381, at 8-9.

would impose on companies that collect and maintain data in paper rather than electronic form. Another commenter cited the costs of providing privacy disclosures and choices in an offline environment.[86]

The Commission notes that consumers face a landscape of virtually ubiquitous collection of their data. Whether such collection occurs online or offline does not alter the consumer's privacy interest in his or her data. For example, the sale of a consumer profile containing the consumer's purchase history from a brick-and-mortar pharmacy or a bookstore would not implicate fewer privacy concerns simply because the profile contains purchases from an offline retailer rather than from an online merchant. Accordingly, the framework applies in all commercial contexts, both online and offline.

4. THE FRAMEWORK APPLIES TO DATA THAT IS REASONABLY LINKABLE TO A SPECIFIC CONSUMER, COMPUTER, OR DEVICE.

The scope issue that generated the most comments, from a wide range of interested parties, was the proposed framework's applicability to "consumer data that can be reasonably linked to a specific consumer, computer, or other device."

A number of commenters supported the proposed framework's application to data that, while not traditionally considered personally identifiable, is linkable to a consumer or device. In particular, several consumer and privacy groups elaborated on the privacy concerns associated with supposedly anonymous data and discussed the decreasing relevance of the personally identifiable information ("PII") label.[87] These commenters pointed to studies demonstrating consumers' objections to being tracked, regardless of whether the tracker explicitly learns a consumer name, and the potential for harm, such as discriminatory pricing based on online browsing history, even without the use of PII.[88]

Similarly, the commenters noted, the ability to re-identify "anonymous" data supports the proposed framework's application to data that can be reasonably linked to a consumer or device. They pointed to incidents, identified in the preliminary staff report, in which individuals were re-identified from publicly released data sets that did not contain PII.[89] One commenter pointed out that certain industries extensively

86 *Comment of National Retail Federation*, cmt. #00419, at 6 (urging FTC to limit privacy framework to online collection of consumer data because applying it to offline collection would be onerous for businesses and consumers).

87 *See Comment of the Center for Democracy & Technology,* cmt. #00469, at 3; *Comment of Consumers Union*, cmt. #00362, at 4-5. In addition, in their comments both AT&T and Mozilla recognized that the distinction between PII and non-PII is blurring. *Comment of AT&T Inc.*, cmt. #00420, at 13; *Comment of Mozilla*, cmt. #00480, at 6.

88 *Comment of Center for Democracy & Technology*, cmt. #00469, at 3 (citing Edward C. Baig, *Internet Users Say, Don't Track Me*, USA TODAY, Dec. 14, 2010, *available at* http://www.usatoday.com/money/advertising/2010-12-14-donottrackpoll14_ST_N.htm); Scott Cleland, *Americans Want Online Privacy – Per New Zogby Poll*, The Precursor Blog (June 8, 2010), http://www.precursorblog.com/content/americans-want-online-privacy-new-zogby-poll); *Comment of Consumers Union*, cmt. #00362, at 4 (discussing the potential for discriminatory pricing (citing Annie Lowery, *How Online Retailers Stay a Step Ahead of Comparison Shoppers*, Wash. Post, Dec. 12, 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/12/11/AR2010121102435.html)).

89 For a brief discussion of such incidents, see FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report,* at 38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

mine data for marketing purposes and that re-identification is a commercial enterprise.[90] This adds to the likelihood of data re-identification.

Some industry commenters also recognized consumers' privacy interest in data that goes beyond what is strictly labeled PII.[91] Drawing on the FTC's roundtables as well as the preliminary staff report, one such commenter noted the legitimate interest consumers have in controlling how companies collect and use aggregated or de-identified data, browser fingerprints,[92] and other types of non-PII.[93] Another company questioned the notion of distinguishing between PII and non-PII as a way to determine what data to protect.[94] Supporting a scaled approach rather than a bright line distinction, this commenter noted that all data derived from individuals deserves some level of protection.[95]

Other commenters representing industry opposed the proposed framework's application to non-PII that can be reasonably linked to a consumer, computer, or device.[96] These commenters asserted that the risks associated with the collection and use of data that does not contain PII are simply not the same as the risks associated with PII. They also claimed a lack of evidence demonstrating that consumers have the same privacy interest in non-PII as they do with the collection and use of PII. Instead of applying the framework to non-PII, these commenters recommended the Commission support efforts to de-identify data.

Overall, the comments reflect a general acknowledgment that the traditional distinction between PII and non-PII has blurred and that it is appropriate to more comprehensively examine data to determine the data's privacy implications.[97] However, some commenters, including some of those cited above, argued that the proposed framework's "linkability" standard is potentially too open-ended to be practical.[98] One industry organization asserted, for instance, that if given enough time and resources, any data may be linkable to an

90 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 4 (citing Julia Angwin & Steve Stecklow, *'Scrapers' Dig Deep for Data on Web*, Wall St. J., Oct. 12, 2010, *available at* http://online.wsj.com/article/SB10001424052748703358504575544381288117888.html); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011).

91 *Comment of Mozilla*, cmt. #00480, at 4-5; *Comment of Google Inc.*, cmt. #00417, at 8.

92 The term "browser fingerprints" refers to the specific combination of characteristics – such as system fonts, software, and installed plugins – that are typically made available by a consumer's browser to any website visited. These characteristics can be used to uniquely identify computers, cell phones, or other devices. Browser fingerprinting does not rely on cookies. *See* Erik Larkin, *Browser Fingerprinting Can ID You Without Cookies*, PCWorld, Jan. 29, 2010, *available at* http://www.pcworld.com/article/188161/browser_fingerprinting_can_id_you_without_cookies.html.

93 *Comment of Mozilla*, cmt. #00480, at 4-5 (citing FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report,* at 36-37 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf).

94 *Comment of Google Inc.*, cmt. #00417, at 8.

95 *Comment of Google Inc.*, cmt. #00417, at 8.

96 *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 13-14; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 13-17.

97 *See Comment of AT&T Inc.*, cmt. #00420, at 13-15; *Comment of Center for Democracy & Technology* (Feb. 18, 2011), cmt. #00469, at 3-4; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 3-4; *Comment of Consumers Union*, cmt. #00362, at 4-5; *Comment of Electronic Frontier Foundation*, cmt. #00400, at 1-4; *Comment of Google Inc.*, cmt. #00417, at 7-8; *Comment of Mozilla*, cmt. #00480, at 4-6; *Comment of Phorm Inc.*, cmt. #00353, at 3-4.

98 *Comment of AT&T Inc.*, cmt. #00420, at 13; Comment of *CTIA - The Wireless Ass'n*, cmt. #00375 at 3-4; *Comment of Google Inc.*, cmt. #00417, at 8; *Comment of Phorm Inc.*, cmt. #00353, at 4.

individual.[99] In addition, commenters stated that requiring the same level of protection for all data would undermine companies' incentive to avoid collecting data that is more easily identified or to take steps to de-identify the data they collect and use.[100] Other commenters argued that applying the framework to data that is potentially linkable could conflict with the framework's privacy by design concept, as companies could be forced to collect more information about consumers than they otherwise would in order to be able to provide those consumers with effective notice, choice, or access.[101] To address these concerns, some commenters proposed limiting the framework to data that is actually linked to a specific consumer, computer, or device.[102]

One commenter recommended that the Commission clarify that the reasonably linkable standard means non-public data that can be linked with *reasonable effort*.[103] This commenter also stated that the framework should exclude data that, through contract or by virtue of internal controls, will not be linked with a particular consumer. Taking a similar approach, another commenter suggested that the framework should apply to data that is reasonably likely to relate to an identifiable consumer.[104] This commenter also noted that a company could commit through its privacy policy that it would only maintain or use data in a de-identified form and that such a commitment would be enforceable under Section 5 of the FTC Act.[105]

The Commission believes there is sufficient support from commenters representing an array of perspectives – including consumer and privacy advocates as well as of industry representatives – for the framework's application to data that, while not yet linked to a particular consumer, computer, or device, may reasonably become so. There is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer, or device even if the individual pieces of data do not constitute PII.[106] Moreover, not only is it possible to re-identify non-PII data through various means,[107] businesses have strong incentives to actually do so.

In response to the comments, to provide greater certainty for companies that collect and use consumer data, the Commission provides additional clarification on the application of the reasonable linkability standard to describe how companies can take appropriate steps to minimize such linkability. Under the final

99 *Comment of GS1*, cmt. #00439, at 2.

100 *Comment of AT&T Inc.*, cmt. #00420, at 13-14; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 4; *Comment of Experian*, cmt. #00398, at 11; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 16.

101 *Comment of United States Council for International Business*, cmt. #00366, at 1; *Comment of Phorm Inc.*, cmt. #00353, at 3.

102 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 4; *Comment of Yahoo! Inc.*, cmt. #00444, at 3-4; *Comment of GS1*, cmt. #00439, at 3.

103 *Comment of AT&T Inc.*, cmt. #00420, at 13.

104 *Comment of Intel Corp.*, cmt. #00246, at 9.

105 *Comment of Intel Corp.,* cmt. #00246, at 9.

106 FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, *Preliminary FTC Staff Report*, 35-38 (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf; *Comment of Center for Democracy & Technology,* cmt. #00469, at 3; *Comment of Statz, Inc.*, cmt. #00377, at 11-12. *See supra* note 89.

107 *See* FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising,* 21-24, 43-45 (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf; Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. Rev. 1814, 1836-1848 (2011).

framework, a company's data would not be reasonably linkable to a particular consumer or device to the extent that the company implements three significant protections for that data.

First, the company must take reasonable measures to ensure that the data is de-identified. This means that the company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device. Consistent with the Commission's approach in its data security cases,[108] what qualifies as a reasonable level of justified confidence depends upon the particular circumstances, including the available methods and technologies. In addition, the nature of the data at issue and the purposes for which it will be used are also relevant. Thus, for example, whether a company publishes data externally affects whether the steps it has taken to de-identify data are considered reasonable. The standard is not an absolute one; rather, companies must take reasonable steps to ensure that data is de-identified.

Depending on the circumstances, a variety of technical approaches to de-identification may be reasonable, such as deletion or modification of data fields, the addition of sufficient "noise" to data, statistical sampling, or the use of aggregate or synthetic data.[109] The Commission encourages companies and researchers to continue innovating in the development and evaluation of new and better approaches to de-identification. FTC staff will continue to monitor and assess the state of the art in de-identification.

Second, a company must publicly commit to maintain and use the data in a de-identified fashion, and not to attempt to re-identify the data. Thus, if a company does take steps to re-identify such data, its conduct could be actionable under Section 5 of the FTC Act.

Third, if a company makes such de-identified data available to other companies – whether service providers or other third parties – it should contractually prohibit such entities from attempting to re-identify the data. The company that transfers or otherwise makes the data available should exercise reasonable oversight to monitor compliance with these contractual provisions and take appropriate steps to address contractual violations.[110]

FTC staff's letter closing its investigation of Netflix, arising from the company's plan to release purportedly anonymous consumer data to improve its movie recommendation algorithm, provides a good illustration of these concepts. In response to the privacy concerns that FTC staff and others raised, Netflix revised its initial plan to publicly release the data. The company agreed to narrow any such release of data to certain researchers. The letter details Netflix's commitment to implement a number of "operational

108 The Commission's approach in data security cases is a flexible one. Where a company has offered assurances to consumers that it has implemented reasonable security measures, the Commission assesses the reasonableness based, among other things, on the sensitivity of the information collected, the measures the company has implemented to protect such information, and whether the company has taken action to address and prevent well-known and easily addressable security vulnerabilities.

109 *See, e.g.*, Cynthia Dwork, *A Firm Foundation for Private Data Analysis*, 54 Comm. of the ACM 86-95 (2011), *available at* http://research.microsoft.com/pubs/116123/dwork_cacm.pdf, and references cited therein.

110 *See In the Matter of Superior Mortg. Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005), *available at*, http://www.ftc.gov/os/caselist/0523136/0523136.shtm (alleging a violation of the GLB Safeguards Rule for, among other things, a failure to ensure that service providers were providing appropriate security for customer information and addressing known security risks in a timely manner).

safeguards to prevent the data from being used to re-identify consumers."[111] If it chose to share such data with third parties, Netflix stated that it would limit access "only to researchers who contractually agree to specific limitations on its use."[112]

Accordingly, as long as (1) a given data set is not reasonably identifiable, (2) the company publicly commits not to re-identify it, and (3) the company requires any downstream users of the data to keep it in de-identified form, that data will fall outside the scope of the framework.[113]

This clarification of the framework's reasonable linkability standard is designed to help address the concern that the standard is overly broad. Further, the clarification gives companies an incentive to collect and use data in a form that makes it less likely the data will be linked to a particular consumer or device, thereby promoting privacy. Additionally, by calling for companies to publicly commit to the steps they take, the framework promotes accountability.[114]

Consistent with the discussion above, the Commission restates the framework's scope as follows.

Final Scope: The framework applies to all commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third parties.

B. PRIVACY BY DESIGN

Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services.

The preliminary staff report called on companies to promote consumer privacy throughout their organizations and at every stage of the development of their products and services. Although many companies already incorporate substantive and procedural privacy protections into their business practices, industry should implement privacy by design more systematically. A number of commenters, including those representing industry, supported staff's call that companies "build in" privacy, with several of these commenters citing to the broad international recognition and adoption of privacy by design.[115] The Commission is encouraged to see broad support for this concept, particularly in light of the increasingly global nature of data transfers.

111 Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy & Identity Prot., FTC, to Reed Freeman, Morrison & Foerster LLP, Counsel for Netflix, 2 (Mar. 12, 2010), *available at* http://www.ftc.gov/os/closings/100312netflixletter.pdf (closing letter).

112 *Id.*

113 To the extent that a company maintains and uses both data that is identifiable and data that it has taken steps to de-identify as outlined here, the company should silo the data separately.

114 A company that violates its policy against re-identifying data could be subject to liability under the FTC Act or other laws.

115 *Comment of Office of the Information and Privacy Commissioner of Ontario*, cmt. #00239, at 2-3; *Comment of Intel Corp.*, cmt. #00246, at 12-13; *Comment of CNIL*, cmt. #00298, at 2-3.

In calling for privacy by design, staff advocated for the implementation of substantive privacy protections – such as data security, limitations on data collection and retention, and data accuracy – as well as procedural safeguards aimed at integrating the substantive principles into a company's everyday business operations. By shifting burdens away from consumers and placing obligations on businesses to treat consumer data in a responsible manner, these principles should afford consumers basic privacy protections without forcing them to read long, incomprehensible privacy notices to learn and make choices about a company's privacy practices. Although the Commission has not changed the proposed "privacy by design" principles, it responds to a number of comments, as discussed below.

1. THE SUBSTANTIVE PRINCIPLES: DATA SECURITY, REASONABLE COLLECTION LIMITS, SOUND RETENTION PRACTICES, AND DATA ACCURACY.

Proposed Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices, and data accuracy.

a. Should Additional Substantive Principles Be Identified?

Responding to a question about whether the final framework should identify additional substantive protections, several commenters suggested incorporating the additional principles articulated in the 1980 OECD Privacy Guidelines.[116] One commenter also proposed adding the "right to be forgotten," which would allow consumers to withdraw data posted online about themselves at any point.[117] This concept has gained importance as people post more information about themselves online without fully appreciating the implications of such data sharing or the persistence of online data over time.[118] In supporting an expansive view of privacy by design, a consumer advocacy group noted that the individual elements and principles of the proposed framework should work together holistically.[119]

In response, the Commission notes that the framework already embodies all the concepts in the 1980 OECD privacy guidelines, although with some updates and changes in emphasis. For example, privacy by design includes the collection limitation, data quality, and security principles. Additionally, the framework's simplified choice and transparency components, discussed below, encompass the OECD principles of purpose specification, use limitation, individual participation, and openness. The framework also adopts the

116 *Comment of CNIL*, cmt. #00298, at 2; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 2; *Comment of World Privacy Forum*, cmt. #00369, at 7; *Comment of Intel Corp.*, cmt. #00246, at 4; *see also* Organisation for Economic Co-operation & Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 1980), *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html (these principles include purpose specification, individual participation, accountability, and principles to govern cross-border data transfers). Another commenter called for baseline legislation based on the Fair Information Practice Principles and the principles outlined in the 1974 Privacy Act. *Comment of Electronic Privacy Information Center*, cmt. #00386, at 17-20.

117 *Comment of CNIL*, cmt. #00298, at 3.

118 The concept of the "right to be forgotten," and its importance to young consumers, is discussed in more detail below in the Transparency Section, *infra* at Section IV.D.2.b.

119 *Comment of Consumers Union*, cmt. #00362, at 1-2, 5-9, 18-19.

OECD principle that companies must be accountable for their privacy practices. Specifically, the framework calls on companies to implement procedures – such as designating a person responsible for privacy, training employees, and ensuring adequate oversight of third parties – to help ensure that they are implementing appropriate substantive privacy protections. The framework also calls on industry to increase efforts to educate consumers about the commercial collection and use of their data and the available privacy tools. In addition, there are aspects of the proposed "right to be forgotten" in the final framework, which calls on companies to (1) delete consumer data that they no longer need and (2) allow consumers to access their data and in appropriate cases suppress or delete it.[120]

All of the principles articulated in the preliminary staff report are intended to work together to shift the burden for protecting privacy away from consumers and to encourage companies to make strong privacy protections the default. Reasonable collection limits and data disposal policies work in tandem with streamlined notices and improved consumer choice mechanisms. Together, they function to provide substantive protections by placing reasonable limits on the collection, use, and retention of consumer data to more closely align with consumer expectations, while also raising consumer awareness about the nature and extent of data collection, use, and third-party sharing, and the choices available to them.

b. Data Security: Companies Must Provide Reasonable Security for Consumer Data.

It is well settled that companies must provide reasonable security for consumer data. The Commission has a long history of enforcing data security obligations under Section 5 of the FTC Act, the FCRA and the GLBA. Since 2001, the FTC has brought 36 cases under these laws, charging that businesses failed to appropriately protect consumers' personal information. Since issuance of the preliminary staff report alone, the Commission has resolved seven data security actions against resellers of sensitive consumer report information, service providers that process employee data, a college savings program, and a social media service.[121] In addition to the federal laws the FTC enforces, companies are subject to a variety of

120 *See In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/index.shtm (requiring Facebook to make inaccessible within thirty days data that a user deletes); *see also* Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011).

121 *In the Matter of Upromise, Inc.*, FTC File No. 102 3116 (Jan. 18, 2012) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/1023116/index.shtm; *In the Matter of ACRAnet, Inc.*, FTC Docket No. C-4331(Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0923088/index.shtm; *In the Matter of Fajilan & Assocs., Inc.*, FTC Docket No. C-4332 (Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0923089/index.shtm; *In the Matter of SettlementOne Credit Corp.*, FTC Docket No. C-4330 (Aug. 17, 2011) (consent order), *available at* http://ftc.gov/os/caselist/0823208/index.shtm; *In the Matter of Lookout Servs., Inc.*, FTC Docket No. C-4326 (June 15, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/102376/index.shtm; *In the Matter of Ceridian Corp.*, FTC Docket No. C-4325 (June 8, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023160/index.shtm; *In the Matter of Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 11, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/0923093/index.shtm.

other federal and state law obligations. In some industries, such as banking, federal regulators have given additional guidance on how to define reasonable security.[122]

The Commission also promotes better data security through consumer and business education. For example, the FTC sponsors OnGuard Online, a website to educate consumers about basic computer security.[123] Since the Commission issued the preliminary staff report there have been over 1.5 million unique visits to OnGuard Online and its Spanish-language counterpart Alerta en Línea. The Commission's business outreach includes general advice about data security as well as specific advice about emerging topics.[124]

The Commission also notes that the private sector has implemented a variety of initiatives in the security area, including the Payment Card Institute Data Security Standards for payment card data, the SANS Institute's security policy templates, and standards and best practices guidelines for the financial services industry provided by BITS, the technology policy division of the Financial Services Roundtable.[125] These standards can provide useful guidance on appropriate data security measures that organizations should implement for specific types of consumer data or in specific industries. The Commission further calls on industry to develop and implement best data security practices for additional industry sectors and other types of consumer data.

Because this issue is important to consumers and because businesses have existing legal and self-regulatory obligations, many individual companies have placed great emphasis and resources on maintaining reasonable security. For example, Google has cited certain security features in its products, including default SSL encryption for Gmail and security features in its Chrome browser.[126] Similarly, Mozilla has noted that

122 *See, e.g.*, Federal Financial Institutions Examination Council ("FFIEC"), *Information Society IT Examination Handbook* (July 2006), *available at* http://ithandbook.ffiec.gov/it-booklets/information-security.aspx; Letter from Richard Spillenkothen, Dir., Div. of Banking Supervision & Regulation, Bd. of Governors of the Fed. Reserve Sys., *SRO1-11: Identity Theft and Pretext Calling* (Apr. 26, 2011), *available at* http://www.federalreserve.gov/boarddocs/srletters/2001/sr0111.htm (guidance on pretexting and identity theft); Securities & Exchange Commission, *CF Disclosure Guidance: Topic No. 2, on Cybersecurity* (Oct. 13, 2011), *available at* http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm; U.S. Small Business Administration, Information Security Guidance, http://www.sba.gov/content/information-security; National Institute of Standards & Technology, Computer Security Division, *Computer Security Resource Center*, *available at* http://csrc.nist.gov/groups/SMA/sbc/index.html; HHS, Health Information Privacy, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html (guidance and educational materials for entities required to comply with the HIPPA Privacy and Security Rules); Centers from Medicare and Medicaid Services, *Educational Materials*, *available at* http://www.cms.gov/EducationMaterials/ (educational materials for HIPPA compliance).

123 FTC, OnGuard Online, http://onguardonline.gov/.

124 *See* FTC, *Protecting Personal Information: A Guide for Business* (Nov. 2011), *available at* http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business; *see generally* FTC, Bureau of Consumer Protection Business Center, Data Security Guidance, *available at* http://business.ftc.gov/privacy-and-security/data-security.

125 *See* PCI Security Standards Council, *PCI SSC Data Security Standards Overview*, *available at* https://www.pcisecuritystandards.org/security_standards/; SANS Institute, *Information Security Policy Templates, available at* http://www.sans.org/security-resources/policies/; BITS, *Financial Services Roundtable BITS Publications*, *available at* http://www.bits.org/publications/index.php; *see also, e.g.*, Better Business Bureau, *Security and Privacy – Made Simpler: Manageable Guidelines to help You Protect Your Customers' Security & Privacy from Identity Theft & Fraud*, *available at* http://www.bbb.org/us/storage/16/documents/SecurityPrivacyMadeSimpler.pdf; National Cyber Security Alliance, *For Business*, http://www.staysafeonline.org/for-business (guidance for small and midsize businesses); Direct Marketing Association, *Information Security: Safeguarding Personal Data in Your Care* (May 2005), *available at* http://www.the-dma.org/privacy/InfoSecData.pdf; Messaging Anti-Abuse Working Group & Anti-Phishing Working Group, *Anti-Phishing Best Practices for ISPs and Mailbox Providers* (July 2006), *available at* http://www.antiphishing.org/reports/bestpracticesforisps.pdf.

126 *Comment of Google Inc.*, cmt. #00417, at 2-3.

its cloud storage system encrypts user data using SSL communication.[127] Likewise, Twitter has implemented encryption by default for users logged into its system.[128] The Commission commends these efforts and calls on companies to continue to look for additional ways to build data security into products and services from the design stage.

Finally, the Commission reiterates its call for Congress to enact data security and breach notification legislation. To help deter violations, such legislation should authorize the Commission to seek civil penalties.

c. Reasonable Collection Limitation: Companies Should Limit Their Collection of Data.

The preliminary staff report called on companies to collect only the data they need to accomplish a specific business purpose. Many commenters expressed support for the general principle that companies should limit the information they collect from consumers.[129] Despite the broad support for the concept, however, many companies argued for a flexible approach based on concerns that allowing companies to collect data only for existing business needs would harm innovation and deny consumers new products and services.[130] One commenter cited Netflix's video recommendation feature as an example of how secondary uses of data can create consumer benefits. The commenter noted that Netflix originally collected information about subscribers' movie preferences in order to send the specific videos requested, but later used this information as the foundation for generating personalized recommendations to its subscribers.[131]

In addition, commenters raised concerns about who decides what a "specific business purpose" is.[132] For example, one purpose for collecting data is to sell it to third parties in order to monetize a service and provide it to consumers for free. Would collecting data for this purpose be a specific business purpose? If not, is the only alternative to charge consumers for the service, and would this result be better for consumers?

As an alternative to limiting collection to accomplish a "specific business purpose," many commenters advocated limiting collection to business purposes *that are clearly articulated*. This is akin to the Fair Information Practice Principle of "purpose specification," which holds that companies should specify to consumers all of the purposes for which information is collected at the time of collection. One commenter supported purpose specification statements in general categories to allow innovation and avoid making privacy policies overly complex.[133]

---

127 *Comment of Mozilla*, cmt. #00480, at 7.

128 *See* Chloe Albanesius, *Twitter Adds Always-On Encryption*, PC Magazine, Feb. 12, 2012, http://www.pcmag.com/article2/0,2817,2400252,00.asp.

129 *See, e.g.*, *Comment of Intel Corp.*, cmt. #00246, at 4-5, 7, 40-41; *Comment of Electronic Frontier Foundation*, cmt. #00400, at 4-6; *Comment of Center for Democracy & Technology*, cmt. #00469, at 4-5; *Comment of Electronic Privacy Information Center*, cmt. #00386, at 18.

130 *See, e.g.*, *Comment of Facebook, Inc.*, cmt. #00413, at 2, 7-8, 18; *Comment of Google Inc.*, cmt. #00417, at 4; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 14-15; *Comment of Intuit, Inc.*, cmt. #00348, at 5, 9; *Comment of TRUSTe*, cmt. #00450, at 9.

131 *Comment of Facebook, Inc.*, cmt. #00413, at 7-8.

132 *See Comment of SAS*, cmt. #00415, at 51; *Comment of Yahoo! Inc.*, cmt. #00444, at 5.

133 *Comment of Yahoo! Inc.*, cmt. #00444, at 5.

The Commission recognizes the need for flexibility to permit innovative new uses of data that benefit consumers. At the same time, in order to protect consumer privacy, there must be some reasonable limit on the collection of consumer data. General statements in privacy policies, however, are not an appropriate tool to ensure such a limit because companies have an incentive to make vague promises that would permit them to do virtually anything with consumer data.

Accordingly, the Commission clarifies the collection limitation principle of the framework as follows: Companies should limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law.[134] For any data collection that is inconsistent with these contexts, companies should make appropriate disclosures to consumers at a relevant time and in a prominent manner – outside of a privacy policy or other legal document. This clarification of the collection limitation principle is intended to help companies assess whether their data collection is consistent with what a consumer might expect; if it is not, they should provide prominent notice and choice. (For a further discussion of this point, see *infra* Section IV.C.2.) This approach is consistent with the Administration's Consumer Privacy Bill of Rights, which includes a Respect for Context principle that limits the use of consumer data to those purposes consistent with the context in which consumers originally disclosed the data.[135]

One example of a company innovating around the concept of privacy by design through collection limitation is the Graduate Management Admission Council ("GMAC"). This entity previously collected fingerprints from individuals taking the Graduate Management Admission Test. After concerns were raised about individuals' fingerprints being cross-referenced against criminal databases, GMAC developed a system that allowed for collection of palm prints that could be used solely for test-taking purposes.[136] The palm print technology is as accurate as fingerprinting but less susceptible to "function creep" over time than the taking of fingerprints, because palm prints are not widely used as a common identifier. GMAC received a privacy innovation award for small businesses for its work in this area.

d. Sound Data Retention: Companies Should Implement Reasonable Data Retention and Disposal Policies.

Similar to the concerns raised about collection limits, many commenters expressed concern about limiting retention of consumer data, asserting that such limits would harm innovation. Trade associations and businesses requested a flexible standard for data retention to allow companies to develop new products

134 This approach mirrors the revised standard for determining whether a particular data practice warrants consumer choice (see *infra* at section IV.C.1.a.) and is consistent with a number of commenters' calls for considering the context in which a particular practice takes place. *See, e.g.*, *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-4; *Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 5; *Comment of TRUSTe*, cmt. #00450, at 3.

135 *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, 15-19, (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. For a further discussion of this point, see *infra* at Section IV.C.1.a.

136 *See* Jay Cline, *GMAC: Navigating EU Approval for Advanced Biomterics*, Inside Privacy Blog (Oct. 15, 2010), https://www.privacyassociation.org/publications/2010_10_20_gmac_navigating_eu_approval_for_advanced_biometrics (explaining GMAC's adoption of palm print technology); *cf.* Kashmir Hill, *Why 'Privacy by Design' is the New Corporate Hotness*, Forbes, July 28, 2011, *available at* http://www.forbes.com/sites/kashmirhill/2011/07/28/why-privacy-by-design-is-the-new-corporate-hotness/.

and other uses of data that provide benefits to consumers.[137] One company raised concerns about prescriptive retention periods, arguing that retention standards instead should be based on business need, the type and location of data at issue, operational issues, and legal requirements.[138] Other commenters noted that retention limits should be sufficiently flexible to accommodate requests from law enforcement or other legitimate business purposes, such as the need of a mortgage banker to retain information about a consumer's payment history.[139] Some commenters suggested that the Commission's focus should be on data security and proper handling of consumer data, rather than on retention limits.[140]

In contrast, some consumer groups advocated specific retention periods. For example, one such commenter cited a proposal made by a consortium of consumer groups in 2009 that companies that collect data for online behavioral advertising should limit their retention of the data to three months and that companies that retained their online behavioral advertising data for only 24 hours may not need to obtain consumer consent for their data collection and use.[141] Others stated that it might be appropriate for the FTC to recommend industry-specific retention periods after a public consultation.[142]

The Commission confirms its conclusion that companies should implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected.[143] Retention periods, however, can be flexible and scaled according to the type of relationship and use of the data; for example, there may be legitimate reasons for certain companies that have a direct relationship with customers to retain some data for an extended period of time. A mortgage company will maintain data for the life of the mortgage to ensure accurate payment tracking; an auto dealer will retain data from its customers for years to manage service records and inform its customers of new offers. These long retention periods help maintain productive customer relationships. This analysis does not, however, apply to all data collection scenarios. A number of commenters noted that online behavioral advertising data often becomes stale quickly and need not be retained long.[144] For example, a consumer researching hotels in a particular city for an upcoming vacation is unlikely to be interested in continuing to see hotel advertisements after the trip is completed. Indefinite retention of data about the consumer's interest in finding a hotel for a particular weekend serves little purpose and could result in marketers sending the consumer irrelevant advertising.

137 *See Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-4, 14; *Comment of American Catalog Mailers Ass'n,* cmt. #000424, at 5; *Comment of IBM*, cmt. #00433, at 4; *Comment of Intuit, Inc.*, cmt. #00348, at 9.

138 *Comment of Verizon*, cmt. #00428, at 10-11.

139 *See, e.g.*, C*omment of CTIA - The Wireless Ass'n*, cmt. #00375, at 14.

140 *Comment of Yahoo! Inc.*, cmt. #00444, at 6; *see also Comment of American Catalog Mailers Ass'n*, cmt. #00424, at 3-4.

141 *Comment of Consumer Federation of America*, cmt. #00358, at 4 (citing *Legislative Primer: Online Behavioral Tracking and Targeting Concerns and Solutions from the Perspective of the Center for Digital Democracy and U.S. PIRG, Consumer Federation of America, Consumers Union, Consumer Watchdog, Electronic Frontier Foundation, Privacy Lives, Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research group, The World Privacy Forum* (Sept. 2009), *available at* http://www.consumerfed.org/elements/www.consumerfed.org/file/OnlinePrivacyLegPrimerSEPT09.pdf).

142 *Comment of Center for Democracy & Technology*, cmt. #00469, at 6 ("Flexible approaches to data retention should not, however, give *carte blanche* to companies to maintain consumer data after it has outlived its reasonable usefulness.").

143 In the alternative, companies may consider taking steps to de-identify the data they maintain, as discussed above.

144 *See Comment of Consumers Union*, cmt. #00362, at 8.

In determining when to dispose of data, as well as limitations on collection described above, companies should also take into account the nature of the data they collect. For example, consider a company that develops an online interactive game as part of a marketing campaign directed to teens. The company should first assess whether it needs to collect the teens' data as part of the game, and if so, how it could limit the data collected, such as by allowing teens to create their own username instead of using a real name and email address. If the company decides to collect the data, it should consider disposing of it even more quickly than it would if it collected adults' data. Similarly, recognizing the sensitivity of data such as a particular consumer's real time location, companies should take special care to delete this data as soon as possible, consistent with the services they provide to consumers.

Although restrictions may be tailored to the nature of the company's business and the data at issue, companies should develop clear standards and train its employees to follow them. Trade associations and self-regulatory groups also should be more proactive in providing guidance to their members about retention and data destruction policies. Accordingly, the Commission calls on industry groups from all sectors – the online advertising industry, online publishers, mobile participants, social networks, data brokers and others – to do more to provide guidance in this area. Similarly, the Commission generally supports the exploration of efforts to develop additional mechanisms, such as the "eraser button" for social media discussed below,[145] to allow consumers to manage and, where appropriate, require companies to delete the information consumers have submitted.

e. Accuracy: Companies should maintain reasonable accuracy of consumers' data.

The preliminary staff report called on companies to take reasonable steps to ensure the accuracy of the data they collect and maintain, particularly if such data could cause significant harm or be used to deny consumers services. Similar to concerns raised about collection limits and retention periods, commenters opposed rigid accuracy standards,[146] and noted that the FCRA already imposes accuracy standards in certain contexts.[147] One commenter highlighted the challenges of providing the same levels of accuracy for non-identifiable data versus data that is identifiable.[148]

To address these challenges, some commenters stated that a sliding scale approach should be followed, particularly for marketing data. These commenters stated that marketing data is not used for eligibility purposes and that, if inaccurate, the only harm a consumer may experience is an irrelevant advertisement.[149] Providing enhanced accuracy standards for marketing data would raise additional privacy and data security concerns,[150] as additional information may need to be added to marketing databases to increase accuracy.[151]

145 See *infra* at Section IV.D.2.b.

146 *See Comment of Experian*, cmt. #00398, at 2.

147 *See Comment of SIFMA*, cmt. #00265, at 4.

148 *Comment of Phorm Inc.*, cmt. #00353, at 4.

149 *Comment of Experian*, cmt. #00398, at 11 (arguing against enhanced standards for accuracy, access, and correction for marketing data); *see also Comment of Yahoo! Inc.*, cmt. #00444, at 6-7.

150 *Id.*

151 *Cf. Comment of Yahoo! Inc.*, cmt. #00444, at 7 (arguing that it would be costly, time consuming, and contrary to privacy objectives to verify the accuracy of user registration information such as gender, age or hometown).

The Commission agrees that the best approach to improving the accuracy of the consumer data companies collect and maintain is a flexible one, scaled to the intended use and sensitivity of the information. Thus, for example, companies using data for marketing purposes need not take special measures to ensure the accuracy of the information they maintain. Companies using data to make decisions about consumers' eligibility for benefits should take much more robust measures to ensure accuracy, including allowing consumers access to the data and the opportunity to correct erroneous information.[152]

Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy.

2. COMPANIES SHOULD ADOPT PROCEDURAL PROTECTIONS TO IMPLEMENT THE SUBSTANTIVE PRINCIPLES.

Proposed Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

In addition to the substantive principles articulated above, the preliminary staff report called for organizations to maintain comprehensive data management procedures, such as designating personnel responsible for employee privacy training and regularly assessing the privacy impact of specific practices, products, and services. Many commenters supported this call for accountability within an organization.[153] Commenters noted that privacy risk assessments promote accountability, and help identify and address privacy issues.[154] One commenter stated that privacy risk assessments should be an ongoing process, and findings should be used to update internal procedures.[155] The Commission agrees that companies should implement accountability mechanisms and conduct regular privacy risk assessments to ensure that privacy issues are addressed throughout an organization.

The preliminary staff report also called on companies to "consider privacy issues systemically, at all stages of the design and development of their products and services." A range of commenters supported the principle of "baking" privacy into the product development process.[156] One commenter stated that this approach of including privacy considerations in the product development process was preferable to requiring

152 See *infra* at Section IV.D.2. The Commission notes that some privacy-enhancing technologies operate by introducing deliberate "noise" into data. The data accuracy principle is not intended to rule out the appropriate use of these methods, provided that the entity using them notifies any recipients of the data that it is inaccurate.

153 *See, e.g.*, *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 2-3; *Comment of Intel Corp.*, cmt. #00246, at 6; *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 3.

154 *Comment of GS1*, cmt. #00439, at 3; *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 6.

155 *Comment of Office of the Information & Privacy Commissioner of Ontario*, cmt. #00239, at 7.

156 *Comment of Intel Corp.*, cmt. #00246, at 6; *Comment of United States Council for International Business*, cmt. #00366, at 2; *Comment of Consumer Federation of America*, cmt. #00358, at 3.

after-the-fact reviews.[157] Another argued that privacy concerns should be considered from the outset, but observed that such concerns should continue to be evaluated as the product, service, or feature evolves.[158]

The Commission's recent settlements with Google and Facebook illustrate how the procedural protections discussed above might work in practice.[159] In both cases, the Commission alleged that the companies deceived consumers about the level of privacy afforded to their data.

The FTC's orders will require the companies to implement a comprehensive privacy program reasonably designed to address privacy risks related to the development and management of new and existing products and services and to protect the privacy and confidentiality of "covered information," defined broadly to mean *any* information the companies collect from or about a consumer.

The privacy programs that the orders mandate must, at a minimum, contain certain controls and procedures, including: (1) the designation of personnel responsible for the privacy program; (2) a risk assessment that, at a minimum, addresses employee training and management and product design and development; (3) the implementation of controls designed to address the risks identified; (4) appropriate oversight of service providers; and (5) evaluation and adjustment of the privacy program in light of regular testing and monitoring.[160] Companies should view the comprehensive privacy programs mandated by these consent orders as a roadmap as they implement privacy by design in their own organizations.

As an additional means of implementing the substantive privacy by design protections, the preliminary staff report advocated the use of privacy-enhancing technologies ("PETs") – such as encryption and anonymization tools – and requested comment on implementation of such technologies. One commenter stressed the need for "privacy-aware design," calling for techniques such as obfuscation and cryptography to reduce the amount of identifiable consumer data collected and used for various products and services.[161] Another stressed that PETs are a better approach in this area than rigid technical mandates.[162]

The Commission agrees that a flexible, technology-neutral approach towards developing PETs is appropriate to accommodate the rapid changes in the marketplace and will also allow companies to innovate on PETs. Accordingly, the Commission calls on companies to continue to look for new ways to protect consumer privacy throughout the life cycle of their products and services, including through the development and deployment of PETs.

Finally, Commission staff requested comment on how to apply the substantive protections articulated above to companies with legacy data systems. Many commenters supported a phase-out period for legacy data systems, giving priority to systems that contain sensitive data.[163] Another commenter suggested that

157 *Comment of Intel Corp.*, cmt. #00246, at 6.

158 *Comment of Zynga Inc.*, cmt. #00459, at 2.

159 Of course, the privacy programs required by these orders may not be appropriate for all types and sizes of companies that collect and use consumer data.

160 *In the Matter of Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/index.shtm.

161 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 5.

162 *Comment of Business Software Alliance*, cmt. #00389, at 7-9.

163 *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 3; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 2; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 14.

imposing strict access controls on legacy data systems until they can be updated would enhance privacy.[164] Although companies need to apply the various substantive privacy by design elements to their legacy data systems, the Commission recognizes that companies need a reasonable transition period to update their systems. In applying the substantive elements to their legacy systems, companies should prioritize those systems that contain sensitive data and they should appropriately limit access to all such systems until they can update them.

Final Principle: Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services.

164 *Comment of Yahoo! Inc.*, cmt. #00444, at 7.

DATA COLLECTION AND DISPOSAL CASE STUDY: MOBILE

The rapid growth of the mobile marketplace illustrates the need for companies to implement reasonable limits on the collection, transfer, and use of consumer data and to set policies for disposing of collected data. The unique features of a mobile phone – which is highly personal, almost always on, and travels with the consumer – have facilitated unprecedented levels of data collection. Recent news reports have confirmed the extent of this ubiquitous data collection. Researchers announced, for example, that Apple had been collecting geolocation data through its mobile devices over time, and storing unencrypted data files containing this information on consumers' computers and mobile devices.[1] The Wall Street Journal has documented numerous companies gaining access to detailed information – such as age, gender, precise location, and the unique ID associated with a particular mobile device – that can then be used to track and predict consumer behavior.[2] Not surprisingly, consumers are concerned: for example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.[3] The Commission calls on companies to limit collection to data they need for a requested service or transaction. For example, a wallpaper app or an app that tracks stock quotes does not need to collect location information.[4]

The extensive collection of consumer information – particularly location information – through mobile devices also heightens the need for companies to implement reasonable policies for purging data.[5] Without data retention and disposal policies specifically tied to the stated business purpose for the data collection, location information could be used to build detailed profiles of consumer movements over time that could be used in ways not anticipated by consumers.[6] Location information is particularly useful for uniquely identifying (or re-identifying) individuals using disparate bits of data.[7] For example, a consumer can use a mobile application on her cell phone to "check in" at a restaurant for the purpose of finding and connecting with friends who are nearby. The same consumer might not expect the application provider to retain a history of restaurants she visited over time. If the application provider were to share that information with third parties, it could reveal a predictive pattern of the consumer's movements thereby exposing the consumer to a risk of harm such as stalking.[8] Taken together, the principles of reasonable collection limitation and disposal periods help to minimize the risks that information collected from or about consumers could be used in harmful or unexpected ways.

With respect to the particular concerns of location data in the mobile context, the Commission calls on entities involved in the mobile ecosystem to work together to establish standards that address data collection, transfer, use, and disposal, particularly for location data. To the extent that location data in particular is collected and shared with third parties, entities should work to provide consumers with more prominent notice and choices about such practices. Although some in the mobile ecosystem provide notice about the collection of geolocation data, not all companies have adequately disclosed the frequency or extent of the collection, transfer, and use of such data.

NOTES

1 *See* Jennifer Valentino-Devries, *Study: iPhone Keeps Tracking Data*, Wall St. J., Apr. 21, 2011, *available at* http://online.wsj.com/article/SB10001424052748704570704576275323811369758.html.

2 *See, e.g.*, Robert Lee Hotz, *The Really Smart Phone*, Wall St. J., Apr. 22, 2011, *available at* http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html (describing how researchers are using mobile data to predict consumers' actions); Scott Thurm & Yukari Iwatane Kane, *Your Apps are Watching You*, Wall St. J., Dec. 18, 2010, *available at* http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html (documenting the data collection that occurs through many popular smartphone apps).

3 *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location*, NielsenWire Blog (Apr. 21, 2011), http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/; *see also* Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* 7 (Mar. 2011), *available at* http://aa-download.avg.com/filedir/other/Smartphone.pdf (reporting that 64% of consumers worry about their location being tracked when using their smartphones).

4 Similarly, the photo-sharing app Path faced widespread criticism for uploading its users' iPhone address books without their consent. *See, e.g.*, Mark Hachman, *Path Uploads Your Entire iPhone Contact List By Default*, PC Magazine, Feb. 7, 2012, *available at* http://www.pcmag.com/article2/0,2817,2399970,00.asp.

5 The Commission is currently reviewing its COPPA Rule, including the application of COPPA to geolocation information. *See* FTC, Proposed Rule and Request for Public Comment, Children's Online Privacy Protection Rule, 76 Fed. Reg. 59,804 (Sept. 15, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-09-27/pdf/2011-24314.pdf.

6 *See* ACLU of Northern California, *Location-Based Services: Time for a Privacy Check-In*, 14-15 (Nov. 2010), *available at* http://dotrights.org/sites/default/files/lbs-white-paper.pdf.

7 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 3.

8 *Cf. U.S. v. Jones*, 565 U.S. 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) (noting that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

C. SIMPLIFIED CONSUMER CHOICE

Baseline Principle: Companies should simplify consumer choice.

As detailed in the preliminary staff report and in submitted comments, many consumers face challenges in understanding the nature and extent of current commercial data practices and how to exercise available choices regarding those practices. This challenge results from a number of factors including: (1) the dramatic increase in the breadth of consumer data collection and use, made possible by an ever-increasing range of technologies and business models; (2) the ability of companies, outside of certain sector-specific laws, to collect and use data without first providing consumer choice; and (3) the inadequacy of typical privacy policies as a means to effectively communicate information about the privacy choices that are offered to consumers.

To reduce the burden on those consumers who seek greater control over their data, the proposed framework called on companies that collect and use consumer data to provide easy-to-use choice mechanisms that allow consumers to control whether their data is collected and how it is used. To ensure that choice is most effective, the report stated that a company should provide the choice mechanism at a time and in a context that is relevant to consumers – generally at the point the company collects the consumer's information. At the same time, however, in recognition of the benefits of various types of data collection and use, the proposed framework identified certain "commonly accepted" categories of commercial data practices that companies can engage in without offering consumer choice.

Staff posed a variety of questions and received numerous comments regarding the proposed framework's simplified consumer choice approach. Two trade organizations argued that the framework should identify those practices for which choice is appropriate rather than making choice the general rule, subject to exceptions for certain practices.[165] The majority of commenters, however, did not challenge the proposed framework's approach of setting consumer choice as the default.[166] Instead, these commenters focused on the practicality of staff's "commonly accepted" formulation.[167] For example, several commenters questioned whether the approach was sufficiently flexible to allow for innovation.[168] Others discussed whether specific practices should fall within the categories enumerated in the preliminary staff report.[169] In addition, numerous commenters addressed the appropriate scope of the first-party marketing category and how to

165 *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8-9.

166 Several commenters expressed support for consumer choice generally. *See*, *e.g.*, *Comment of Center for Democracy & Technology*, cmt. #00469, at 11-12; *Comment of Consumer Federation of America,* cmt. #00358, at 6-12. One governmental agency, for instance, expressly supported a general rule requiring consumer consent for the collection and any use of their information with only limited exceptions. *Comment of Department of Veteran Affairs*, cmt. #00479, at 5. Another commenter, supporting consumer choice, emphasized the importance of offering opportunities for choice beyond a consumer's initial transaction. *Comment of Catalog Choice,* cmt. #00473, at 10-18.

167 *Comment of Center for Democracy & Technology,* cmt. #00469, at 8-11; *Comment of Consumer Federation of America*, cmt. #00358, at 6-10.

168 *Comment of Computer and Communications Industry Ass'n*, cmt. #00434, at 16; *Comment of BlueKai*, cmt. #00397, at 3-4; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 5-7; *U.S. Chamber of Commerce*, cmt. #00452, at 5; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 23-24; *Comment of Yahoo! Inc.*, cmt. #00444, at 9-10.

169 *Comment of Phorm Inc.*, cmt. #00353, at 5; *Comment of Verizon,* cmt. #00428, at 11-13.

define specific business models. With respect to those practices that fall outside the "commonly accepted" categories, commenters also addressed the mechanics of providing choice at the relevant time and what types of practices require enhanced choice.

Consistent with the discussion and analysis set forth below, the Commission retains the proposed framework's simplified choice model. Establishing consumer choice as a baseline requirement for companies that collect and use consumer data, while also identifying certain practices where choice is unnecessary, is an appropriately balanced model. It increases consumers' control over the collection and use of their data, preserves the ability of companies to innovate new products and services, and sets clear expectations for consumers and industry alike. In order to better foster innovation and take into account new technologies and business models, however, the Commission is providing further clarification of the framework's simplified choice concept.

1. PRACTICES THAT DO NOT REQUIRE CHOICE.

Proposed Principle: Companies do not need to provide choice before collecting and using consumers' data for commonly accepted practices, such as product fulfillment.

The preliminary staff report identified five categories of data practices that companies can engage in without offering consumer choice, because they involve data collection and use that is either obvious from the context of the transaction or sufficiently accepted or necessary for public policy reasons. The categories included: (1) product and service fulfillment; (2) internal operations; (3) fraud prevention; (4) legal compliance and public purpose; and (5) first-party marketing. In response to the comments received, the Commission revises its approach to focus on the context of the consumer's interaction with a company, as discussed below.

a. General Approach to "Commonly Accepted" Practices.

While generally supporting the concept that choice is unnecessary for certain practices, a variety of commenters addressed the issue of whether the list of "commonly accepted" practices was too broad or too narrow.[170] A number of industry commenters expressed concern that the list of practice categories was too narrow and rigid. These commenters stated that, by enumerating a list of specific practices, the proposed framework created a bright-line standard that freezes in place current practices and potentially could harm innovation and restrict the development of new business models.[171] In addition, the commenters asserted that notions of what is "commonly accepted" can change over time with the development of new ways to collect or use data. They also stated that line-drawing in this context could stigmatize business practices that fall outside of the "commonly accepted" category and place companies that engage in them at a competitive

170 *Comment of AT&T Inc.,* cmt. #00420, at 18-22; *Comment of Center for Democracy & Technology*, cmt. #00469, at 8-11; *Comment of Consumers Union*, cmt. #00362, at 9-12; *Comment of Consumer Federation of America*, cmt. #00358, at 6-10; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 23-25.

171 *Comment of Computer and Communications Industry Ass'n*, cmt. #00434, at 16; *Comment of BlueKai*, cmt. #00397, at 4; *Comment of Retail Industry Leaders Ass'n,* cmt. #00352, at 6-7; *Comment of Yahoo! Inc.*, cmt. #00444, at 9-12; *Comment of National Cable & Telecommunications Ass'n,* cmt. #00432, at 23-24.

disadvantage. To resolve these concerns, commenters called on the Commission to provide guidance on how future practices relate to the "commonly accepted" category.[172] Similarly, one commenter suggested that the practices identified in the preliminary staff report should serve as illustrative guidelines rather than an exhaustive and final list.[173]

Commenters also supported adding additional practices or clarifying that the "commonly accepted" category includes certain practices. Some industry commenters suggested, for example, expanding the concept of fraud prevention to include preventing security attacks, "phishing,"[174] and spamming or to protect intellectual property.[175] Other recommendations included adding analytical data derived from devices that are not tied to individuals, such as smart grid data used for energy conservation and geospatial data used for mapping, surveying or providing emergency services.[176] With respect to online behavioral advertising in particular, some trade associations recommended clarifying that the "commonly accepted" category of practices includes the use of IP addresses and third-party cookie data when used for purposes such as "frequency capping," "attribution measurement," and similar inventory or delivery measurements and to prevent click fraud.[177]

More generally, some commenters discussed the "repurposing" of existing consumer data to develop new products or services. For example, one company supported expanding the "internal operations" category to include the practice of product and service improvement.[178] One commenter recommended treating any uses of data that consumers would "reasonably expect under the circumstances" as commonly accepted.[179] Another noted that, whether a new use of consumer data should be considered commonly accepted would depend upon a variety of factors, including the extent to which the new use is consistent with previously defined uses.[180]

In contrast to the calls for expanding the "commonly accepted" practice categories to cover various practices, a number of consumer and privacy organizations advocated for a more restrictive approach to determining the practices that do not require consumer choice. Although agreeing that choice is not necessary for product and service fulfillment, one commenter stated that most of the other practices enumerated in the proposed framework – including internal operations, fraud prevention, and legal compliance and public purpose – were vague and required additional description. The commenter called on

172 *Comment of eBay*, cmt. #00374, at 6-7; *Comment of Phorm Inc.*, cmt. #00353, at 5.

173 *See Comment of AT&T Inc.*, cmt. #00420, at 18.

174 Phishing uses deceptive spam that appears to be coming from legitimate, well-known sources to trick consumers into divulging sensitive or personal information, such as credit card numbers, other financial data, or passwords.

175 *See Comment of Microsoft Corp.*, cmt. #00395, at 8 (security attacks, phishing schemes, and spamming); *Comment of Business Software Alliance*, cmt. #00389, at 5-6 (security access controls and user and employee authentication, cybercrime and fraud prevention and detection, protecting and enforcing intellectual property and trade secrets).

176 *See Comment of IBM,* cmt. #00433, at 5 (energy conservation); *Comment of Management Ass'n for Private Programming Surveyors*, cmt. #00205, at 2-3 (mapping, surveying or providing emergency services).

177 *See Comment of Online Publishers Ass'n*, cmt. #00315, at 5 (frequency capping, click fraud); *Comment of Interactive Advertising Bureau*, cmt. #00388, at 9 (attribution measurement).

178 *See Comment of AT&T Inc.*, cmt. #00420, at 18-19.

179 *See Comment of Microsoft Corp.*, cmt. #00395, at 8.

180 *See Comment of Future of Privacy Forum*, cmt. #00341, at 5.

the Commission to define these terms as narrowly as possible so that they would not become loopholes used to undermine consumer privacy.[181]

One privacy advocate expressed reservations about the breadth of the "internal operations" category of practices – specifically, the extent to which it could include product improvement and website analytics. This commenter stated that, if viewed broadly, product improvement could justify, for example, a mobile mapping application collecting precise, daily geolocation data about its customers and then retaining the data long after providing the service for which the data was necessary. Similarly, this commenter noted that companies potentially could use analytics programs to create very detailed consumer profiles to which many consumers might object, without offering them any choice. This commenter recommended that the Commission revise the proposed framework's internal operations category to make it consistent with the "operational purpose" language contained in H.R. 611 from the 112th Congress, which would include, among other things, "basic business functions such as accounting, inventory and supply chain management, quality assurance, and internal auditing."[182]

The Commission believes that for some practices, the benefits of providing choice are reduced – either because consent can be inferred or because public policy makes choice unnecessary. However, the Commission also appreciates the concerns that the preliminary staff report's definition of "commonly accepted practices" may have been both under-inclusive and over-inclusive. To the extent the proposed framework was interpreted to establish an inflexible list of specific practices, it risked undermining companies' incentives to innovate and develop new products and services to consumers, including innovative methods for reducing data collection while providing valued services. On the other hand, companies could read the definition so broadly that virtually any practice could be considered "commonly accepted."

The standard should be sufficiently flexible to allow for innovation and new business models but also should cabin the types of practices that do not require consumer choice. To strike that balance, the Commission refines the standard to focus on the *context of the interaction* between a business and the consumer. This new "context of the interaction" standard is similar to the concept suggested by some commenters that the need for choice should depend on reasonable consumer expectations,[183] but is intended to provide businesses with more concrete guidance. Rather than relying solely upon the inherently subjective test of consumer expectations, the revised standard focuses on more objective factors related to the consumer's relationship with a business. Specifically, whether a practice requires choice turns on the extent

181 *See Comment of Consumer Federation of America*, cmt. #00358, at 6.

182 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 8-9 (citing BEST PRACTICES Act, H.R. 611, 112th Congress § 2(5)(iii) (2011).

183 *See Comment of Microsoft Corp.*, cmt. #00395, at 8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 23-26; *Comment of Pharmaceutical Research & Manufacturers of America*, cmt. #00477, at 13.

to which the practice is consistent with the context of the transaction or the consumer's existing relationship with the business, or is required or specifically authorized by law.[184]

The purchase of an automobile from a dealership illustrates how this standard could apply. In connection with the sale of the car, the dealership collects personal information about the consumer and his purchase. Three months later, the dealership uses the consumer's address to send him a coupon for a free oil change. Similarly, two years after the purchase, the dealership might send the consumer notice of an upcoming sale on the type of tires that came with the car or information about the new models of the car. In this transaction the data collection and subsequent use is consistent with the context of the transaction and the consumer's relationship with the car dealership. Conversely, if the dealership sells the consumer's personal information to a third-party data broker that appends it to other data in a consumer profile to sell to marketers, the practice would not be consistent with the car purchase transaction or the consumer's relationship with the dealership.

Although the Commission has revised the standard for evaluating when choice is necessary, it continues to believe that the practices highlighted in the preliminary staff report – fulfilment, fraud prevention, internal operations, legal compliance and public purpose, and most first-party marketing[185] – provide illustrative guidance regarding the types of practices that would meet the revised standard and thus would not typically require consumer choice. Further, drawing upon the recommendations of several commenters,[186] the Commission agrees that the fraud prevention category would generally cover practices designed to prevent security attacks or phishing; internal operations would encompass frequency capping and similar advertising inventory metrics; and legal compliance and public purpose would cover intellectual property protection or using location data for emergency services.[187] It should be noted, however, that even within these categories there may be practices that are inconsistent with the context of the interaction standard and thus warrant consumer choice. For instance, there may be contexts in which the "repurposing" of data to improve existing products or services would exceed the internal operations concept. Thus, where a product improvement involves additional sharing of consumer data with third parties, it would no longer be an "internal operation" consistent with the context of the consumer's interaction with a company. On the

184 As noted above, focusing on the context of the interaction is consistent with the Respect for Context principle in the Consumer Privacy Bill of Rights proposed by the White House. *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, App. A. (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The Respect for Context principle requires companies to limit their use of consumer data to purposes that are consistent with the company's relationship with the consumer and with the context in which the consumer disclosed the data, unless the company is legally required to do otherwise. If a company will use data for other purposes it must provide a choice at a prominent point, outside of the privacy policy.

185 *See supra* at Section IV.C.1.

186 *See supra* note 175.

187 With respect to use of geolocation data for mapping, surveying or similar purposes, if the data cannot reasonably be linked to a specific consumer, computer, or device, a company collecting or using the data would not need to provide a consumer choice mechanism. Similarly, if a company takes reasonable measures to de-identify smart grid data and takes the other steps outlined above, the company would not be obligated to obtain consent before collecting or using the data. See *supra* Section IV.A.4.

other hand, product improvements such as a website redesign or a safety improvement would be the type of "internal operation" that is generally consistent with the context of the interaction.[188]

b. First-Party Marketing Generally Does Not Require Choice, But Certain Practices Raise Special Concerns.

The preliminary staff report's questions regarding first-party marketing generated a large number of comments. As discussed, the Commission has revised the standard for determining whether a practice requires consumer choice but believes that most first-party marketing practices are consistent with the consumer's relationship with the business and thus do not necessitate consumer choice. Nevertheless, as a number of the commenters discussed, there are certain practices that raise special concerns and therefore merit additional analysis and clarification.

(i) Companies Must Provide Consumers With A Choice Whether To Be Tracked Across Other Parties' Websites.

Commenters raised questions about companies and other services that have first-party relationships with consumers, but may have access to behavioral activity data that extends beyond the context of that first-party relationship. For example, in response to the question in the preliminary staff report regarding the use of deep packet inspection ("DPI"),[189] a number of commenters cited the ability of ISPs to use DPI to monitor and track consumers' movements across the Internet and use the data for marketing.[190] There appeared to be general consensus among the commenters that, based on the potential scope of the tracking, an ISP's use of DPI for marketing purposes is distinct from other forms of marketing practices by companies that have a first-party relationship with consumers, and thus at a minimum requires consumer choice.[191]

Similarly, commenters cited the use of "social plugins" – such as the Facebook "Like" button – that allow social media services to track consumers across every website that has installed the plugin.[192] The commenter stated that, as with DPI, consumers would not expect social media sites to track their visits to other websites or that the profiles created from such tracking could be used for marketing.

188 Moreover, even if a given practice does not necessitate consumer choice, the framework's other elements – *e.g.*, data collection limits and disposal requirements, increased transparency – would still apply, thereby preventing a company from exploiting these categories.

189 Deep packet inspection ("DPI") refers to the ability of ISPs to analyze the information, comprised of data packets, that traverses their networks when consumers use their services.

190 *See Comment of AT&T Inc.*, cmt. #00420, at 21-22 & n.34; *Comment of Berlin Commissioner for Data Protection & Freedom of Information*, cmt. #00484, at 2-3; *Comment of Computer & Communications Industry Ass'n*, cmt. #00434, at 15; *Comment of Phorm Inc.*, cmt. #00353, App. A at 3-4; *Comment of U.S. Public Policy Council of the Ass'n for Computing Machinery*, cmt. #00431, at 6.

191 *See Comment of Phorm Inc.*, cmt. #00353, App. A at 3-4; *Comment of Center for Democracy & Technology*, cmt. #00469, at 14-15; *Comment of AT&T Inc.*, cmt. #00420, at 21-22 & n.34.

192 *See Comment of Consumer Federation of America*, cmt. #00358, at 8 (citing Justin Brookman, *Facebook Pressed to Tackle Lingering Privacy Concerns*, Center for Democracy & Technology (June 16, 2010), *available at* https://www.cdt.org/blogs/justin-brookman/facebook-pressed-tackle-lingering-privacy-concerns); *Comment of Berkeley Center for Law & Technology*, cmt. #00347, at 8; *see also* Arnold Roosendaal, *Facebook Tracks and Traces Everyone: Like This!*, (Nov. 30, 2010), *available at* http://papers.ssrn.com/so13/papers.cfm?abstract_id=1717563 (detailing how Facebook tracks consumers through the Like button, including non-Facebook members and members who have logged out of their Facebook accounts); Nik Cubrilovic, *Logging Out Of Facebook Is Not Enough*, New Web Order (Sept. 25, 2011), http://nikcub.appspot.com/posts/logging-out-of-facebook-is-not-enough.

The Commission agrees that where a company that has a first-party relationship with a consumer for delivery of a specific service but also tracks the consumer's activities across other parties' websites, such tracking is unlikely to be consistent with the context of the consumer's first-party relationship with the entity. Accordingly, under the final framework, such entities should not be exempt from having to provide consumers with choices. This is true whether the entity tracks consumers through the use of DPI, social plug-ins, http cookies, web beacons, or some other type of technology.[193]

As an example of how this standard can apply, consider a company with multiple lines of business, including a search engine and an ad network. A consumer has a "first-party relationship" with the company when using the search engine. While it may be consistent with this first-party relationship for the company to offer contextual ads on the search engine site, it would be inconsistent with the first-party search engine relationship for the company to use its third-party ad network to invisibly track the consumer across the Internet.

To use another example, many online retailers engage in the practice of "retargeting," in which the retailer delivers an ad to a consumer on a separate website based on the consumer's previous activity on the retailer's website.[194] Because the ad is tailored to the consumer's activity on the retailer's website, it could be argued that "retargeting" is a first-party marketing practice that does not merit consumer choice. However, because it involves tracking the consumer from the retailer's website to a separate site on which the retailer is a third party and communicating with the consumer in this new context, the Commission believes that the practice of retargeting is inconsistent with the context of consumer's first-party interaction with the retailer. Thus, where an entity has a first-party relationship with a consumer on its own website, and it engages in third-party tracking of the consumer across other websites the entity should provide meaningful choice to the consumer.

(ii) Affiliates Are Third Parties Unless The Affiliate Relationship Is Clear to Consumers.

Several trade organizations stated that first-party marketing should include the practice of data sharing among all of a particular entity's corporate affiliates and subsidiaries.[195] In contrast, a number of commenters – including individual companies and consumer advocates – took a more limited approach that would treat affiliate sharing as a first-party practice only if the affiliated companies share a trademark, are commonly-branded, or the affiliated relationship is otherwise reasonably clear to consumers.[196] One consumer advocate also suggested restricting data sharing to commonly-branded affiliates in the same line of business so that the data would be used in a manner that is consistent with the purpose for which the first party collected it.[197]

193 See *infra* at Section IV.C.2.d. (discussing special concerns that arise by comprehensive tracking by large platform providers).

194 For example, a consumer visits an online sporting goods retailer, looks at but does not purchase running shoes, and then visits a different website to read about the local weather forecast. A first party engages in retargeting if it delivers an ad for running shoes to the consumer on the third-party weather site.

195 *See Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 24.

196 *See Comment of Yahoo! Inc.*, cmt. #00444, at 11; *Comment of IBM*, cmt. #00433, at 6; *Comment of AT&T Inc.*, cmt. #00420, at 20; *Comment of Catalog Choice*, cmt. #00473, at 10; *Comment of Consumers Union*, cmt. #00362, at 10-11.

197 *See Comment of Consumers Union*, cmt. #00362, at 10-11.

The Commission maintains the view that affiliates are third parties, and a consumer choice mechanism is necessary unless the affiliate relationship is clear to consumers. Common branding is one way of making the affiliate relationship clear to consumers. By contrast, where an affiliate relationship is hidden – such as between an online publisher that provides content to consumers through its website and an ad network that invisibly tracks consumers' activities on the site – marketing from the affiliate would not be consistent with a transaction on, or the consumer's relationship with, that website. In this scenario consumers should receive a choice about whether to allow the ad network to collect data about their activities on the publisher's site.

(iii) Cross-Channel Marketing Is Generally Consistent with the Context of a Consumer's Interaction with a Company.

A variety of commenters also discussed the issue of whether the framework should require choice for cross-channel marketing, *e.g.*, where a consumer makes an in-store purchase and receives a coupon – not at the register, but in the mail or through a text message. These commenters stated that the framework should not require choice when a first party markets to consumers through different channels, such as the Internet, email, mobile apps, texts, or in the offline context.[198] In support of this conclusion, one commenter stated that restricting communications from a first party to the initial means of contact would impose costs on business without any consumer benefits.[199]

The Commission agrees that the first-party marketing concept should include the practice of contacting consumers across different channels. Regardless of the particular means of contact, receipt of a message from a company with which a consumer has interacted directly is likely to be consistent with the consumer's relationship with that company.[200] At the same time, as noted above, if an offline or online retailer tracks a customer's activities on a third-party website, this is unlikely to be consistent with the customer's relationship with the retailer; thus, choice should be required.

(iv) Companies Should Implement Measures to Improve The Transparency of Data Enhancement.

A large number of commenters discussed whether the practice of data enhancement, by which a company appends data obtained from third-party sources to information it collects directly from consumers, should require choice. Some of these commenters specifically objected to allowing companies to enhance data without providing consumers choice about the practice.[201]

For example, one academic organization characterized data enhancement without consumer choice as "trick[ing]" consumers into participating in their own profiling for the benefit of companies.[202] As

198 *See Comment of Yahoo! Inc.*, cmt. #00444, at 10; *Comment of IBM*, cmt. #00433, at 6; *Comment of AT&T Inc.*, cmt. #00420, at 20; *Comment of Catalog Choice*, cmt. #00473, at 9-10; *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 16; *Comment of Interactive Advertising Bureau*, cmt. #00388, at 8.

199 *See Comment of American Catalog Mailers Ass'n,* cmt. #00424, at 7.

200 Such marketing communications would, of course, still be subject to any existing restrictions, including the CAN-SPAM Act, 15 U.S.C. §§ 7701-7713 (2010).

201 *See Comment of Consumer Federation of America*, cmt. #00358, at 10; *Comment of Consumers Union*, cmt. #00362, at 11.

202 *Comment of Berkeley Center for Law & Technology*, cmt. #00347, at 9-10.

companies develop new means for collecting data about individuals, this commenter stated, consumers should have more tools to control data collection, not fewer.[203]

Similarly, a consumer organization explained that consumers may not anticipate that the companies with which they have a relationship can obtain additional data about them from other sources, such as social networking sites, and use the data for marketing.[204] This commenter concluded that requiring companies to provide choice will necessitate better explanations of the practice, which will lead to improved consumer understanding.

Other stakeholders also raised concerns about data enhancement absent consumer choice. One company focused on the practice of enhancing online cookie data or IP addresses with offline identity data and stated that such enhancement should be subject to consumer choice.[205] In addition, a data protection authority stated that consumers are likely to expect choice where the outcome of data enhancement could negatively affect the consumer or where the sources of data used for enhancement would be unexpected to the consumer.[206]

Alternatively, a number of industry commenters opposed requiring consumer choice for data enhancement in connection with first-party marketing. These commenters described data enhancement as a routine and longstanding practice that allows businesses to better understand and serve their consumers.[207] Commenters enumerated a variety of benefits from the availability and use of third-party data, including: development of new or more relevant products and services; ensuring the accuracy of databases; reducing barriers to small firms seeking to enter markets; helping marketers identify the best places to locate retail stores; and reducing irrelevant marketing communications.[208]

One commenter noted that requiring content publishers such as newspapers to offer consumer choice before buying information from non-consumer-facing data brokers would impose logistical and financial challenges that would interfere with publishers' ability to provide relevant content or sell the advertising to support it.[209] Other commenters claimed that, where the data used for enhancement comes from third-party sources, it was likely subject to choice at the point of collection from the consumer and therefore providing additional choice is unnecessary.[210] Taking a similar approach, one company noted that the third-party source of the data should be responsible for complying with the framework when it shares data, and the recipient should be responsible for any subsequent sharing of the enhanced data.[211]

---

203 *Id.*, at 8-10 (describing Williams-Sonoma's collection of consumers' zip codes in *Pineda v. Williams-Sonoma Stores, Inc.*, 246 P.3d 612 (Cal. 2011)).

204 *Comment of Consumer Federation of America*, cmt. #00358, at 10.

205 *See Comment of Phorm Inc.*, cmt. #00353, at 5.

206 *See Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 3.

207 *See Comment of Newspaper Ass'n of America,* cmt. #00383, at 7-8; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 24-26; *Comment of Experian*, cmt. #00398, at 5-6; *Comment of Magazine Publishers of America*, cmt. #00332, at 4; *Consumer Data Industry Ass'n,* cmt. #00363, at 2-3.

208 *Comment of Experian*, cmt. #00398, at 6; *see Comment of Newspaper Ass'n of America*, cmt. #00383, at 6-8.

209 *Comment of Newspaper Ass'n of America*, cmt. #00383, at 7-8.

210 *Comment of Experian*, cmt. #00398, at 9 (citing the Direct Marketing Association's Guidelines for Ethical Business Practice); *Comment of Magazine Publishers of America,* cmt. #00332, at 5-6.

211 *Comment of Microsoft Corp.*, cmt. #00395, at 8.

The issue of whether a first-party marketer should provide choice for data enhancement is particularly challenging because the practice involves two separate and distinct types of consumer data collection. One involves the consumer-to-business transfer of data – for instance, where an online retailer collects information directly from the consumer by tracking the products the consumer purchased in the store or looked at while visiting the retailer's website. The other involves a business-to-business transfer of data – such as where retailer purchases consumer data from a non-consumer-facing data broker.

As to the first type of data collection, for the reasons discussed above, if the first party does not share information with third parties or track consumers across third-party websites, the practice would be consistent with the context of the consumer's interaction with the company.[212] Therefore, the framework would not call for a consumer choice mechanism. In contrast, because the second type of data collection involves the transfer of data from one business to another and does not directly involve the consumer (and therefore is typically unknown to the consumer), it is unlikely to be consistent with a transaction or relationship between the consumer and the first party. The Commission nevertheless recognizes that it would be impractical to require the first-party marketer to offer a choice mechanism when it appends data from third-party sources to the data it collects directly from its consumers. As discussed in the comments, such a requirement would impose costs and logistical problems that could preclude the range of benefits that data enhancement facilitates.

Instead, full implementation of the framework's other components should address the privacy concerns that commenters raised about data enhancement. First, companies should incorporate privacy by design concepts, including limiting the amount of data they collect from consumers and third parties alike to accomplish a specific business purpose, reducing the amount of time they retain such data, and adopting reasonable security measures. The framework also calls for consumer choice where a company shares with a third party the data it collects from a consumer. Thus, consumers will have the ability to control the flow of their data to third parties who might sell the data to others for enhancement. In addition, companies should improve the transparency of their practices by disclosing that they engage in data enhancement and educating consumers about the practice, identifying the third-party sources of the data, and providing a link or other contact information so the consumer can contact the third-party source directly. Finally, to further protect consumer privacy, the Commission recommends that first parties that obtain marketing data for enhancement should take steps to encourage their third-party data broker sources to increase their own transparency, including by participating in a centralized data broker website, discussed further below, where consumers could learn more information about data brokers and exercise choices.[213] The first parties may also consider contractually requiring their data broker sources to take these steps.

212 See *supra* Section IV.C.1.b.(i).

213 The concept of such a website is discussed, *infra*, Section IV.D.2.a.

DATA ENHANCEMENT CASE STUDY: FACIAL RECOGNITION SOFTWARE

Facial recognition technology[1] enables the identification of an individual based on his or her distinct facial characteristics. While this technology has been used in experiments for over thirty years, until recently it remained costly and limited under real world conditions.[2] However, steady improvements in the technology combined with increased computing power have shifted this technology out of the realm of science fiction and into the marketplace. As costs have decreased and accuracy improved, facial recognition software has been incorporated into a variety of commercial products. Today it can be found in online social networks and photo management software, where it is used to facilitate photo-organizing,[3] and in mobile apps where it is used to enhance gaming.[4]

This surge in the deployment of facial recognition technology will likely boost the desire of companies to use data enhancement by offering yet another means to compile and link information about an individual gathered through disparate transactions and contexts. For instance, social networks such as Facebook and LinkedIn, as well as websites like Yelp and Amazon, all encourage users to upload profile photos and make these photos publicly available. As a result, vast amounts of facial data, often linked with real names and geographic locations, have been made publicly available. A recent paper from researchers at Carnegie Mellon University illustrated how they were able to combine readily available facial recognition software with data mining algorithms and statistical re-identification techniques to determine in many cases an individual's name, location, interests, and even the first five digits of the individual's Social Security number, starting with only the individual's picture.[5]

Companies could easily replicate these results. Today, retailers use facial *detection* software in digital signs to analyze the age and gender of viewers and deliver targeted advertisements.[6] Facial detection does not uniquely identify an individual. Instead, it detects human faces and determines gender and approximate age range. In the future, digital signs and kiosks placed in supermarkets, transit stations, and college campuses could capture images of viewers and, through the use of facial *recognition* software, match those faces to online identities, and return advertisements based on the websites specific individuals have visited or the publicly available information contained in their social media profiles. Retailers could also implement loyalty programs, ask users to associate a photo with the account, then use the combined data to link the consumer to other online accounts or their in-store actions. This would enable the retailer to glean information about the consumer's purchase habits, interests, and even movements,[7] which could be used to offer discounts on particular products or otherwise market to the consumer.

The ability of facial recognition technology to identify consumers based solely on a photograph, create linkages between the offline and online world, and compile highly detailed dossiers of information, makes it especially important for companies using this technology to implement privacy by design concepts and robust choice and transparency policies. Such practices should include reducing the amount of time consumer information is retained, adopting reasonable security measures, and disclosing to consumers that the facial data they supply may be used to link them to information from third parties or publicly available sources. For example, if a digital sign uses data enhancement to deliver targeted advertisements to viewers, it should immediately delete the data after the consumer has walked away. Likewise, if a kiosk is used to invite shoppers to register for a store loyalty program, the shopper should be informed that the photo taken by the kiosk camera and associated with the account may be combined with other data to market discounts and offers to the shopper. If a company received the data from other sources, it should disclose the sources to the consumer.

NOTES

1 The Commission held a facial recognition workshop on December 8, 2011. *See* FTC Workshop, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), http://www.ftc.gov/bcp/workshops/facefacts/.

2 *See* Alessandro Acquisti *et al.*, *Faces of Facebook: Privacy in the Age of Augmented Reality*, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

3 *See* Justin Mitchell, *Making Photo Tagging Easier*, The Facebook Blog (June 30, 2011, 5:16 PM), https://blog.facebook.com/blog.php?post=467145887130; Matt Hickey, *Picasa Refresh Brings Facial Recognition*, TechCrunch (Sept. 2, 2008), http://techcrunch.com/2008/09/02/picasa-refresh-brings-facial-recognition/.

4 *See* Tomio Geron, V*iewdle Launches 'Third Eye' Augmented Reality Game*, Forbes, June 22, 2011, *available at* http://www.forbes.com/sites/tomiogeron/2011/06/22/viewdle-lauches-third-eye-augmented-reality-game/.

5 *See* Alessandro Acquisti *et al.*, *Faces of Facebook: Privacy in the Age of Augmented Reality*, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

6 *See* Shan Li & David Sarno, *Advertisers Start Using Facial Recognition to Tailor Pitches*, L.A. Times, Aug. 21, 2011, *available at* http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821.

7 For instance, many consumers use services such as Foursquare which allow them to use their mobile phone to "check in" at a restaurant to find friends who are nearby. *See* Foursquare, About Foursquare, https://foursquare.com/about.

(v) Companies Should Generally Give Consumers a Choice Before Collecting Sensitive Data for First-Party Marketing.

Commenters addressed whether companies that collect sensitive data[214] for their own marketing should offer consumer choice. A number of privacy and consumer organizations asserted that even where a business collects data in a first-party setting, any marketing based on sensitive data should require the consumer's affirmative express consent.[215] These commenters stated that the use of sensitive data for marketing could cause embarrassment for consumers or lead to various types of discriminatory conduct, including denial of benefits or being charged higher prices. One such commenter also noted that heightened choice for sensitive data is consistent with the FTC staff's Self-Regulatory Principles for Online Behavioral Advertising ("2009 OBA Report").[216]

Rather than always requiring consent, an industry trade association pushed for a more flexible approach to the use of sensitive data in first-party marketing.[217] This commenter stated that the choice analysis should depend upon the particular context and circumstances in which the data is used. The commenter noted that, for example, with respect to sensitive location data, where a consumer uses a wireless service to find nearby restaurants and receive discounts, the consumer implicitly understands his location data will be used and consent can be inferred.

The Commission agrees with the commenters who stated that affirmative express consent is appropriate when a company uses sensitive data for any marketing, whether first- or third-party. Although, as a general rule, most first-party marketing presents fewer privacy concerns, the calculus changes when the data is sensitive. Indeed, when health or children's information is involved, for example, the likelihood that data misuse could lead to embarrassment, discrimination, or other harms is increased. This risk exists regardless of whether the entity collecting and using the data is a first party or a third party that is unknown to the consumer. In light of the heightened privacy risks associated with sensitive data, first parties should provide a consumer choice mechanism at the time of data collection.[218]

At the same time, the Commission believes this requirement of affirmative express consent for first-party marketing using sensitive data should be limited. Certainly, where a company's business model is *designed to target* consumers based on sensitive data – including data about children, financial and health information, Social Security numbers, and certain geolocation data – the company should seek affirmative express consent before collecting the data from those consumers.[219] On the other hand, the risks to consumers may not justify the potential burdens on general audience businesses that *incidentally collect* and use sensitive

214 The Commission defines as sensitive, at a minimum, data about children, financial and health information, Social Security numbers, and certain geolocation data, as discussed below. See *infra* Section IV.C.2.e.(ii).

215 *Comment of Center for Democracy & Technology*, cmt. #00469, at 10; *Comment of Consumer Federation of America*, cmt. #00358, at 8-9; *Comment of Consumers Union*, cmt. #00362, at 12-13.

216 *See Comment of Center for Democracy & Technology*, cmt. #00469 at 10 (citing FTC, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising*, 43-44 (2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf).

217 *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 4-6.

218 Additional discussion regarding the necessary level of consent for the collection or use of sensitive data, as well as other practices that raise special privacy considerations, is set forth below. See *infra* Section IV.C.2.e.(ii).

219 These categories of sensitive data are discussed further below. See *infra* Section IV.C.2.e.(ii).

information. For example, the Commission has previously noted that online retailers and services such as Amazon.com and Netflix need not provide choice when making product recommendations based on prior purchases. Thus, if Amazon.com were to recommend a book related to health or financial issues based on a prior purchase on the site, it need not provide choice. However, if a health website is designed to target people with particular medical conditions, that site should seek affirmative express consent when marketing to consumers.

Final Principle: Companies do not need to provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law.

2. FOR PRACTICES INCONSISTENT WITH THE CONTEXT OF THEIR INTERACTION WITH CONSUMERS, COMPANIES SHOULD GIVE CONSUMERS CHOICES.

Proposed Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data.

For those practices for which choice is contemplated, the proposed framework called on companies to provide choice at a time and in a context in which the consumer is making a decision about his or her data. In response, commenters discussed a number of issues, including the methods for providing just in time choice, when "take-it-or-leave-it" choice may be appropriate, how to respond to the call for a Do Not Track mechanism that would allow consumers to control online tracking, and the contexts in which affirmative express consent is necessary.

The Commission adopts the proposed framework's formulation that choice should be provided at a time and in a context in which the consumer is making a decision about his or her data. The Commission also adds new language addressing when a company should seek a consumer's affirmative express consent.

a. Companies Should Provide Choices At a Time and In a Context in Which the Consumer Is Making a Decision About His or Her Data.

The call for companies to provide a "just in time" choice generated numerous comments. Several consumer organizations as well as industry commenters stressed the importance of offering consumer choice at the time the consumer provides – and the company collects or uses – the data at issue and pointed to examples of existing mechanisms for providing effective choice.[220] One commenter stated that in order to make choice mechanisms meaningful to consumers, companies should incorporate them as a feature of a product or service rather than as a legal disclosure.[221] Using its vendor recommendation service as an example, this commenter suggested incorporating a user's sharing preferences into the sign-up process instead of setting such preferences as a default that users can later adjust and personalize. Another

220 *See Comment of Consumer Federation of America*, cmt. #00358, at 10; *Comment of Center for Democracy & Technology*, cmt. #00469, at 23-24; *Comment of AT&T Inc.,* cmt. #00420, at 22-23; *Comment of Phorm Inc.*, cmt. #00353, at 9-10.

221 *Comment of AT&T Inc.*, cmt. #00420, at 22-23.

commenter stated that choice options should occur in a "time-appropriate manner" that takes into account the "functional and aesthetic context" of the product or service.[222]

Others raised concerns about the practicality of providing choice prior to the collection or use of data in different contexts.[223] For instance, a number of commenters discussed the offline retail context and noted that cashiers are typically unqualified to communicate privacy information or to discuss data collection and use practices with customers.[224] One commenter further discussed the logistical problems with providing such information at the point of sale, citing consumer concerns about ease of transaction and in-store wait times.[225] Other commenters described the impracticality of offering and obtaining advance consent in an offline mail context, such as a magazine subscription card or catalogue request that a consumer mails to a fulfillment center.[226] In the online context, one commenter expressed concern that "pop-up" choice mechanisms complicate or clutter the user experience, which could lead to choice "fatigue."[227] Another commenter noted that where data collection occurs automatically, such as in the case of online behavioral advertising, obtaining consent before collection could be impractical.[228]

One theme that a majority of the commenters addressing this issue articulated is the need for flexibility so that companies can tailor the choice options to specific business models and contexts.[229] Rather than a rigid reliance on advance consent, commenters stated that companies should be able to provide choice before collection, close to the time of collection, or a time that is convenient to the consumer.[230] The precise method should depend upon context, the sensitivity of the data at issue, and other factors.[231] Citing its own best practices guidance, one trade organization recommended that the Commission focus not on the precise mechanism for offering choice, but on whether the consent is informed and based on sufficient notice.[232]

The Commission appreciates the concerns that commenters raised about the timing of providing choices. Indeed, the proposed framework was not intended to set forth a "one size fits all" model for designing consumer choice mechanisms. Staff instead called on companies to offer clear and concise choice

222 *Comment of Center for Democracy & Technology*, cmt. #00469, at 11.

223 *See Comment of Microsoft Corp.*, cmt. #00395, at 8-10, 14; *Comment of SIFMA*, cmt. #00265, at 5-6; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 8-10.

224 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 8; *Comment of Experian*, cmt. #00398, at 9.

225 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 8.

226 *See Comment of Magazine Publishers of America*, cmt. #00332, at 4 (noting that the "blow-in cards" in magazines often used to solicit new subscriptions have very limited space, and including lengthy disclosures on these cards could render them unreadable); *Comment of American Catalogue Mailers Ass'n,* cmt. #00424, at 7.

227 *See Comment of Retail Industry Leaders Ass'n*, cmt. #00352 at 7; *see also Comment of Experian*, cmt. #00398, at 9 (noting that the proposed changes in notice and choice procedures would be inconvenient for consumers and would damage the consumer experience).

228 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 8.

229 *Comment of Microsoft Corp.*, cmt. #00395, at 2; *Comment of AT&T Inc.*, cmt. #00420 at 3, 7; *Comment of Consumers Union*, cmt. #00362, at 5, 11-12; *Comment of Consumer Federation of America,* cmt. #00358, at 10.

230 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 9.

231 *Comment of Facebook, Inc.*, cmt. #00413, at 10; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 9; *see also Comment of Experian*, cmt. #00398, at 9 (generally disputing the need for "just-in-time" notice, but acknowledging that it might be justified for the transfer to non-affiliated third parties of sensitive information for marketing purposes).

232 *See Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 10 (describing the form of consent outlined in the CTIA's "Best Practices and Guidelines for Location-Based Services").

mechanisms that are easy to use and are delivered at a time and in a context that is relevant to the consumer's decision about whether to allow the data collection or use. Precisely how companies in different industries achieve these goals may differ depending on such considerations as the nature or context of the consumer's interaction with a company or the type or sensitivity of the data at issue.

In most cases, providing choice before or at the time of collection will be necessary to gain consumers' attention and ensure that the choice presented is meaningful and relevant. If a consumer is submitting his or her data online, the consumer choice could be offered, for example, directly adjacent to where the consumer is entering his or her data. In other contexts, the choice might be offered immediately upon signing up for a service, as in the case of a social networking website.

In some contexts, however, it may be more practical to communicate choices at a later point. For example, in the case of an offline retailer, the choice might be offered close to the time of a sale, but in a manner that will not unduly interfere with the transaction. This could include communicating the choice mechanism through a sales receipt or on a prominent poster at the location where the transaction takes place. In such a case, there is likely to be a delay between when the data collection takes place and when the consumer is able to contact the company in order to exercise any choice options. Accordingly, the company should wait for a disclosed period of time before engaging in the practices for which choice is being offered.[233] The Commission also encourages companies to examine the effectiveness of such choice mechanisms periodically to determine whether they are sufficiently prominent, effective, and easy to use.

Industry is well positioned to design and develop choice mechanisms that are practical for particular business models or contexts, and that also advance the fundamental goal of giving consumers the ability to make informed and meaningful decisions about their privacy. The Commission calls on industry to use the same type of creativity industry relies on to develop effective marketing campaigns and user interfaces for consumer choice mechanisms. One example of such a creative approach is the online behavioral advertising industry's development of a standardized icon and text that is embedded in targeted advertisements. The icon and text are intended to communicate that the advertising may rely on data collected about consumers. They also serve as a choice mechanism to allow the consumer to exercise control over the delivery of such ads.[234] Even though in most cases, cookie placement has already occurred, the in-ad disclosure provides a logical "teachable moment" for the consumer who is making a decision about his or her data.[235]

b. Take-it-or-Leave-it Choice for Important Products or Services Raises Concerns When Consumers Have Few Alternatives.

Several commenters addressed whether it is appropriate for a company to make a consumer's use of its product or service contingent upon the consumer's acceptance of the company's data practices. Two industry

233 The FTC recognizes that incorporating this delay period may require companies to make programming changes to their systems. As noted above, in the discussion of legacy data systems, see *supra* at Section IV.B.2., these changes may take time to implement.

234 As noted in Section IV.C.2.c., industry continues to consider ways to make the icon and opt out mechanism more usable and visible for consumers.

235 *But see Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 29 (criticizing visibility of the icon to consumers).

commenters suggested that "take-it-or-leave-it" or "walk away" choice is common in many business models, such as retail and software licensing, and companies have a right to limit their business to those who are willing to accept their policies.[236] Another commenter stated that preventing companies from offering take-it-or-leave-it choice might be unconstitutional under the First Amendment.[237] Other commenters, however, characterized walk away choice as generally inappropriate.[238] Some argued that the privacy framework should prevent companies from denying consumers access to goods or services, including website content, where consumers choose to limit the collection or use of their data.[239]

Most of the commenters that addressed this issue took a position somewhere in between.[240] In determining whether take-it-or-leave-it choice is appropriate, these commenters focused on three main factors. First, they noted that there must be adequate competition, so that the consumer has alternative sources to obtain the product or service in question.[241] Second, they stated that the transaction must not involve an essential product or service.[242] Third, commenters stated that the company offering take-it-or-leave-it choice must clearly and conspicuously disclose the terms of the transaction so that the consumer is able to understand the value exchange. For example, a company could clearly state that in exchange for receiving a service at "no cost," it collects certain information about your activity and sells it to third parties.[243] Expanding upon this point, commenters stressed that to ensure consumer understanding of the nature of the take-it-or-leave-it bargain, the disclosure must be prominent and not buried within a privacy policy.[244]

The Commission agrees that a "take it or leave it" approach is problematic from a privacy perspective, in markets for important services where consumers have few options.[245] For such products or services, businesses should not offer consumers a "take it or leave it" choice when collecting consumers' information in a manner inconsistent with the context of the interaction between the business and the consumer. Take,

236 *Comment of Performance Marketing Ass'n*, cmt. #00414, at 6; *Comment of Business Software Alliance,* cmt. #00389, at 11-12.

237 *Comment of Tech Freedom*, cmt. #00451, at 17.

238 *Comment of Consumer Federation of America*, cmt. #00358, at 11; *Comment of ePrio, Inc.*, cmt. #00267, at 4-5.

239 *Comment of Consumer Federation of America*, cmt. #00358, at 11; *see also Comment of Consumers Union,* cmt. #00362, at 12 (urging that consumers who choose to restrict sharing of their PII with unknown third parties should not be punished for that choice).

240 *See, e.g., Comment of Center for Democracy & Technology*, cmt. #00469, at 13 (stating that it has no objection to take-it-or-leave-it approaches, provided there is competition and the transaction does not involve essential services); *Comment of Microsoft Corp.*, cmt. #00395, at 10 (stating that take-it-or-leave-it choice is appropriate provided the "deal" is made clear to the consumer); *Comment of the Information Commissioner's Office of the UK,* cmt. #00249, at 4 (stating that take-it-or-leave-it choice would be inappropriate where the consumer has no real alternative but to use the service); *Comment of Reed Elsevier, Inc.*, cmt. #00430, at 11 (stating that while acceptable for the websites of private industry, websites that provide a public service and may be the single source of certain information, such as outsourced government agency websites, should not condition their use on take-it-or-leave-it terms).

241 *Comment of Center for Democracy & Technology*, cmt. #00469, at 13; *Comment of the Information Commissioner's Office of the UK,* cmt. #00249, at 4.

242 *Comment of Center for Democracy & Technology,* cmt. #00469, at 13; *Comment of Reed Elsevier, Inc.*, cmt. #00430, at 11.

243 *Comment of Microsoft Corp.*, cmt. #00395, at 10; *see also Comment of Center for Democracy & Technology,* cmt. #00469, at 13 (stating that the terms of the bargain should be clearly and conspicuously disclosed).

244 *Comment of TRUSTe*, cmt. #00450, at 11; *see also Comment of Center for Democracy & Technology*, cmt. #00469, at 13 (stating that terms should be "transparent and fairly presented").

245 This Report is not intended to reflect Commission guidance regarding Section 5's prohibition on unfair methods of competition.

for example, the purchase of an important product that has few substitutes, such as a patented medical device. If a company offered a limited warranty for the device only in exchange for the consumer's agreeing to disclose his or her income, religion, and other highly-personal information, the consumer would not have been offered a meaningful choice and a take-it-or-leave approach would be inappropriate.

Another example is the provision of broadband Internet access. As consumers shift more aspects of their daily lives to the Internet – shopping, interacting through social media, accessing news, entertainment, and information, and obtaining government services – broadband has become a critical service for many American consumers. When consumers have few options for broadband service, the take-it-or-leave-it approach becomes one-sided in favor of the service provider. In these situations, the service provider should not condition the provision of broadband on the customer's agreeing to, for example, allow the service provider to track all of the customer's online activity for marketing purposes. Consumers' privacy interests ought not to be put at risk in such one-sided transactions.

With respect to less important products and services in markets with sufficient alternatives, take-it-or-leave-it choice can be acceptable, provided that the terms of the exchange are transparent and fairly disclosed – *e.g.*, "we provide you with free content in exchange for collecting information about the websites you visit and using it to market products to you." Under the proper circumstances, such choice options may result in lower prices or other consumer benefits, as companies develop new and competing ways of monetizing their business models.

c. Businesses Should Provide a Do Not Track Mechanism To Give Consumers Control Over the Collection of Their Web Surfing Data.

Like the preliminary staff report, this report advocates the continued implementation of a universal, one-stop choice mechanism for online behavioral tracking, often referred to as Do Not Track. Such a mechanism should give consumers the ability to control the tracking of their online activities.

Many commenters discussed the progress made by industry in developing such a choice mechanism in response to the recommendations of the preliminary staff report and the 2009 OBA Report, and expressed support for these self-regulatory initiatives.[246] These initiatives include the work of the online advertising industry over the last two years to simplify disclosures and improve consumer choice mechanisms; efforts by the major browsers to offer new choice mechanisms; and a project of a technical standards body to

246 *See, e.g.*, *Comment of American Ass'n of Advertising Agencies et. al*, cmt. #00410, at 3 (describing the universal choice mechanisms used in the coalition's Self-Regulatory Principles for Online Behavioral Advertising Program); *Comment of BlueKai*, cmt. #00397, at 3 (describing its development of the NAI Opt-Out Protector for Firefox); *Comment of Computer & Communications Industry Ass'n*, cmt. #00434, at 17 (describing both company-specific and industry-wide opt-out mechanisms currently in use); *Comment of Direct Marketing Ass'n, Inc.*, cmt. #00449, at 3 (stating that the Self-Regulatory Principles for Online Behavioral Advertising Program addresses the concerns that motivate calls for a "Do-Not-Track" mechanism); *Comment of Facebook, Inc.*, cmt. #00413, at 13 (describing behavioral advertising opt-out mechanisms developed by both browser makers and the advertising industry); *Comment of Future of Privacy Forum*, cmt. #00341, at 2-4 (describing the development of a browser-based Do-Not-Track header and arguing that the combined efforts of browser companies, ad networks, consumers, and government are likely to result in superior choice mechanisms); *Comment of Google, Inc.*, cmt. #00417, at 5 (describing its Ad Preferences Manager and Keep My Opt-Outs tools); *Comment of Interactive Advertising Bureau,* cmt. #00388, at 5-7 (describing the Self-Regulatory Principles for Online Behavioral Advertising Program); *Comment of Microsoft Corp.*, cmt. #00395, at 11-14 (describing a variety of browser-based and ad network-based choice tools currently available); *Comment of U.S. Chamber of Commerce,* cmt. #00452, at 5-6 (describing a variety of browser-based and ad network-based choice tools currently available).

standardize opt outs for online tracking.[247] A number of commenters, however, expressed concerns that existing mechanisms are still insufficient. Commenters raised questions about the effectiveness and comprehensiveness of existing mechanisms for exercising choice and the legal enforceability of such mechanisms.[248] Due to these concerns, some commenters advocated for legislation mandating a Do Not Track mechanism.[249]

The Commission commends recent industry efforts to improve consumer control over behavioral tracking and looks forward to final implementation. As industry explores technical options and implements self-regulatory programs, and Congress examines Do Not Track, the Commission continues to believe that in order to be effective, any Do Not Track system should include five key principles. First, a Do Not Track system should be implemented universally to cover all parties that would track consumers. Second, the choice mechanism should be easy to find, easy to understand, and easy to use. Third, any choices offered should be persistent and should not be overridden if, for example, consumers clear their cookies or update their browsers. Fourth, a Do Not Track system should be comprehensive, effective, and enforceable. It should opt consumers out of behavioral tracking through any means and not permit technical loopholes.[250] Finally, an effective Do Not Track system should go beyond simply opting consumers out of receiving targeted advertisements; it should opt them out of collection of behavioral data for all purposes other than those that would be consistent with the context of the interaction (*e.g.*, preventing click-fraud or collecting de-identified data for analytics purposes).[251]

Early on the companies that make web browsers stepped up to the challenge to give consumers choice about how they are tracked online, sometimes known as the "browser header" approach. The browser header is transmitted to all types of entities, including advertisers, analytics companies, and researchers, that track consumers online. Just after the FTC's call for Do Not Track, Microsoft developed a system to let users of Internet Explorer prevent tracking by different companies and sites.[252] Mozilla introduced a Do Not Track privacy control for its Firefox browser that an impressive number of consumers have adopted.[253]

247 *See supra* at Section II.C.1.

248 *Comment of American Civil Liberties Union*, cmt. #00425, at 12; *Comment of Center for Digital Democracy and U.S. PIRG,* cmt. #00338, at 28; *Comment of Consumer Federation of America*, cmt. #00358, at 13; *Comment of Consumers Union*, cmt. #00362, at 14; *see also Comment of World Privacy Forum,* cmt. #00369, at 3 (noting prior failures of self-regulation in the online advertising industry).

249 *E.g., Comment of Consumers Union*, cmt. #00362, at 14; *Comment of World Privacy Forum*, cmt. #00369, at 3.

250 For example, consumers may believe they have opted out of tracking if they block third-party cookies on their browsers; yet they may still be tracked through Flash cookies or other mechanisms. The FTC recently brought an action against a company that told consumers they could opt out of tracking by exercising choices through their browsers; however, the company used Flash cookies for such tracking, which consumers could not opt out of through their browsers. *In the Matter of ScanScout, Inc.*, FTC Docket No. C-4344 (Dec. 21, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023185/111221scanscoutdo.pdf.

251 Such a mechanism should be different from the Do Not Call program in that it should not require the creation of a "Registry" of unique identifiers, which could itself cause privacy concerns.

252 *Comment of Microsoft Corp.*, cmt. #00395, at 12.

253 *Comment of Mozilla*, cmt. #00480, at 2; Alex Fowler, *Do Not Track Adoption in Firefox Mobile is 3x Higher than Desktop*, Mozilla Privacy Blog, (Nov. 2, 2011), http://blog.mozilla.com/privacy/2011/11/02/do-not-track-adoption-in-firefox-mobile-is-3x-higher-than-desktop/.

Apple subsequently included a similar Do Not Track control in Safari.[254] Google has taken a slightly different approach – providing consumers with a tool that persistently opts them out of most behavioral advertising.[255]

In another important effort, the online advertising industry, led by the DAA, has implemented a behavioral advertising opt-out program. The DAA's accomplishments are notable: it has developed a notice and choice mechanism through a standard icon in ads and on publisher sites; deployed the icon broadly, with over 900 billion impressions served each month; obtained commitments to follow the self-regulatory principles from advertisers, ad networks, and publishers that represent close to 90 percent of the online behavioral advertising market; and established an enforcement mechanism designed to ensure compliance with the principles.[256] More recently, the DAA addressed one of the long-standing criticisms of its approach – how to limit secondary use of collected data so that the consumer opt out extends beyond simply blocking targeted ads to the collection of information for other purposes. The DAA has released new principles that include limitations on the collection of tracking data and prohibitions on the use or transfer of the data for employment, credit, insurance, or health care eligibility purposes.[257] Just as important, the DAA recently moved to address some persistence and usability criticisms of its icon-based opt out by committing to honor the tracking choices consumers make through their browser settings.[258]

At the same time, the W3C Internet standards-setting body has gathered a broad range of stakeholders to create an international, industry-wide standard for Do Not Track. The group includes a wide variety of stakeholders, including DAA members; other U.S. companies; international companies; industry groups; and public-interest groups. The W3C group has done admirable work to flesh out the details required to make a Do Not Track system practical in both desktop and mobile settings. The group has issued two public working drafts of its standards. Some important details remain to be filled in, and the Commission encourages all of the stakeholders to work within the W3C group to resolve these issues.

While more work remains to be done on Do Not Track, the Commission believes that the developments to date are significant and provide an effective path forward. The advertising industry, through the DAA, has committed to deploy browser-based technologies for consumer control over online tracking, alongside its ubiquitous icon program. The W3C process, thanks in part to the ongoing participation of DAA member companies, has made substantial progress toward specifying a consensus consumer choice system for tracking

254 Nick Wingfield, *Apple Adds Do-Not-Track Tool to New Browser*, Wall St. J. Apr. 13, 2011, *available at* http://online.wsj.com/article/SB10001424052748703551304576261272308358858.html.

255 *Comment of Google Inc.*, cmt. #00417, at 5.

256 Peter Kosmala, *Yes, Johnny Can Benefit From Transparency & Control*, Self-Regulatory Program for Online Behavioral Advertising, http://www.aboutads.info/blog/yes-johnny-can-benefit-transparency-and-control (Nov. 3, 2011); *see also* Press Release, Digital Advertising Alliance, White House, DOC and FTC Commend DAA's Self-Regulatory Program to Protect Consumers Online Privacy, (Feb. 23, 2012), *available at* http://www.aboutads.info/resource/download/DAA%20White%20House%20Event.pdf.

257 Digital Advertising Alliance, *About Self-Regulatory Principles for Multi-Site Data* (Nov. 2011), *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf.

258 Press Release, Digital Advertising Alliance, DAA Position on Browser Based Choice Mechanism (Feb. 22, 2012), *available at* http://www.aboutads.info/resource/download/DAA.Commitment.pdf.

that is practical and technically feasible.[259] The Commission anticipates continued progress in this area as the DAA members and other key stakeholders continue discussions within the W3C process to work to reach consensus on a Do Not Track system in the coming months.

d. Large Platform Providers That Can Comprehensively Collect Data Across the Internet Present Special Concerns.

As discussed above, even if a company has a first-party relationship with a consumer in one setting, this does not imply that the company can track the consumer for purposes inconsistent with the context of the interaction across the Internet, without providing choice. This principle applies fully to large platform providers such as ISPs, operating systems, and browsers, who have very broad access to a user's online activities.

For example, the preliminary staff report sought comment on the use of DPI for marketing purposes. Many commenters highlighted the comprehensive nature of DPI.[260] Because of the pervasive tracking that DPI allows, these commenters stated that its use for marketing should require consumers' affirmative express consent.[261] Privacy concerns led one commenter to urge the Commission to oppose DPI and hold workshops and hearings on the issue.[262] Another commenter argued that a lack of significant competition among broadband providers argues in favor of heightened requirements for consumer choice before ISPs can use DPI for marketing purposes.[263]

Two major ISPs emphasized that they do not use DPI for marketing purposes and would not do so without first seeking their customers' affirmative express consent.[264] They cautioned against singling out DPI as a practice that presents unique privacy concerns, arguing that doing so would unfairly favor certain technologies or business models at the expense of others. One commenter also stated that the framework should not favor companies that use other means of tracking consumers.[265] This commenter noted that various technologies – including cookies – allow companies to collect and use information in amounts similar to that made possible through DPI, and the framework's principles should apply consistently based

259 A system practical for both businesses and consumers would include, for users who choose to enable Do Not Track, significant controls on the collection and use of tracking data by third parties, with limited exceptions such as security and frequency capping. As noted above, first-party sharing with third parties is not consistent with the context of the interaction and would be subject to choice. Do Not Track is one way for users to express this choice.

260 *Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15; *Comment of Center for Democracy & Technology*, cmt. #00469, at 14-15.

261 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 14; *Comment of Phorm Inc.*, cmt. #00353, at 5; *see also Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15 (urging that heightened requirements for consumer choice apply for the use of DPI); *Comment of Online Trust Alliance*, cmt. #00299, at 6 ("The use of DPI and related technologies may also be permissible when consumers have the ability to opt-in and receive appropriate and proportional quantifiable benefits in return.")

262 *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 37.

263 *Comment of Computer and Communications Industry Ass'n*, cmt. #00233, at 15.

264 *Comment of AT&T Inc.*, cmt. #00420, at 21; *see also Comment of Verizon*, cmt. #00428, at 7 n.6. Likewise, a trade association of telecommunications companies represented that ISPs have not been extensively involved in online behavioral advertising. *See Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 33.

265 *See Comment of Verizon*, cmt. #00428, at 7.

on the type of information collected and how it is used.[266] Rather than isolating a specific technology, commenters urged the Commission to focus on the type of data collected and how it is used.[267]

ISPs serve as a major gateway to the Internet with access to vast amounts of unencrypted data that their customers send or receive over the ISP's network. ISPs are thus in a position to develop highly detailed and comprehensive profiles of their customers – and to do so in a manner that may be completely invisible. In addition, it may be difficult for some consumers to obtain alternative sources of broadband Internet access, and they may be inhibited from switching broadband providers for reasons such as inconvenience or expense. Accordingly, the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection.[268]

At the same time, the Commission agrees that any privacy framework should be technology neutral. ISPs are just one type of large platform provider that may have access to all or nearly all of a consumer's online activity. Like ISPs, operating systems and browsers may be in a position to track all, or virtually all, of a consumer's online activity to create highly detailed profiles.[269] Consumers, moreover, might have limited ability to block or control such tracking except by changing their operating system or browser.[270] Thus, comprehensive tracking by any such large platform provider may raise serious privacy concerns.

The Commission also recognizes that the use of cookies and social widgets to track consumers across unrelated websites may create similar privacy issues.[271] However, while companies such as Google and Facebook are expanding their reach rapidly, they currently are not so widespread that they could track a consumer's every movement across the Internet.[272] Accordingly, although tracking by these entities warrants consumer choice, the Commission does not believe that such tracking currently raises the same level of privacy concerns as those entities that can comprehensively track all or virtually of a consumer's online activity.

These are complex and rapidly evolving areas, and more work should be done to learn about the practices of all large platform providers, their technical capabilities with respect to consumer data, and their current and expected uses of such data. Accordingly, Commission staff will host a workshop in the second half

266 *Id.* at 7-8.

267 *See, e.g.*, *Comment of Internet Commerce Coalition*, cmt. #00447, at 10; *Comment of KINDSIGHT*, cmt. #00344, at 7-8 ; *Comment of National Cable & Telecommunications Ass'n,* cmt. #00432, at 36; *Comment of Verizon*, cmt. #00428, at 7-8.

268 This discussion does not apply to ISPs' use of DPI for network management, security, or other purposes consistent with the context of a consumer's interaction with their ISP.

269 This discussion is not meant to imply that ISPs, operating systems, or browsers are currently building these profiles for marketing purposes.

270 ISPs, operating systems, and browsers have different access to users' online activity. A residential ISP can access unencrypted traffic from all devices currently located in the home. An operating system or browser, on the other hand, can access all traffic regardless of location and encryption, but only from devices on which the operating system or browser is installed. Desktop users have the ability to change browsers to avoid monitoring, but mobile users have fewer browser options.

271 A social widget is a button, box, or other possibly interactive display associated with a social network that is embedded into another party's website.

272 BrightEdge, *Social Share Report: Social Adoption Among Top Websites*, 3-4 (July 2011), *available at* http://www.brightedge.com/resfiles/brightedge-report-socialshare-2011-07.pdf (reporting that by mid-2011, the Facebook Like button appeared on almost 11% of top websites' front pages and Google's +1 button appeared on 4.5% of top websites' front pages); *see also* Justin Osofsky, *After f8: Personalized Social Plugins Now on 100,000+ Sites*, Facebook Developer Blog (May 11, 2010, 9:15 AM), http://developers.facebook.com/blog/post/382/.

of 2012 to explore the privacy issues raised by the collection and use of consumer information by a broad range of large platform providers such as ISPs, operating systems, browsers, search engines, and social media platforms as well as how competition issues may bear on appropriate privacy protection.[273]

e. Practices Requiring Affirmative Express Consent.

Numerous commenters focused on whether certain data collection and use practices warrant a heightened level of consent – *i.e.*, affirmative express consent.[274] These practices include (1) making material retroactive changes to a company's privacy representations; and (2) collection of sensitive data. These comments and the Commission's analysis are discussed here.

(i) Companies Should Obtain Affirmative Express Consent Before Making Material Retroactive Changes To Privacy Representations.

The preliminary staff report reaffirmed the Commission's bedrock principle that companies should provide prominent disclosures and obtain affirmative express consent before using data in a manner materially different than claimed at the time of collection.[275]

Although many commenters supported the affirmative express consent standard for material retroactive changes,[276] some companies called for an opt-out approach for material retroactive changes, particularly for changes that provide benefits to consumers.[277] One example cited was the development of Netflix's personalized video recommendation feature using information that Netflix originally collected in order to send consumers the videos they requested.[278] Other companies sought to scale the affirmative consent requirement according to the sensitivity of the data and whether the data is personally identifiable.[279] Many commenters sought clarification on when a change is material – for example, whether a change in data retention periods would be a material change requiring heightened consent.[280] One company posited

273 *See Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 37 (recommending FTC hold a workshop to address DPI).

274 Companies may seek "affirmative express consent" from consumers by presenting them with a clear and prominent disclosure, followed by the ability to opt in to the practice being described. Thus, for example, requiring the consumer to scroll through a ten-page disclosure and click on an "I accept" button would not constitute affirmative express consent.

275 In the preliminary report, this principle appeared under the heading of "transparency." *See, e.g.*, *In the Matter of Gateway Learning Corp.*, FTC Docket No. C-4120 (Sept. 10, 2004) (consent order) (alleging that Gateway violated the FTC Act by applying material changes to a privacy policy retroactively), *available at* http://www.ftc.gov/os/caselist/0423047/040917do0423047.pdf; *see also* FTC, *Self-Regulatory Principles for Online Behavioral Advertising* (Feb. 2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf (noting the requirement that companies obtain affirmative express consent before making material retroactive changes to their privacy policies).

276 *See Comment of Consumers Union*, cmt. #00362, at 17; *Comment of Future of Privacy Forum*, cmt. #00341, at 5; *Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 21.

277 *See Comment of Facebook, Inc.*, cmt. #00413, at 11; *see also Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 12; *Comment of AT&T Inc.*, cmt. #00420, at 29-30; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 30-31.

278 *Comment of Facebook, Inc.*, cmt. #00413, at 8.

279 *See Comment of AT&T Inc.*, cmt. #00420, at 30; *Comment of Phorm Inc.*, cmt. #00353, at 1.

280 *See Comment of Future of Privacy Forum*, cmt. #00341, at 4; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 12; *Comment of Microsoft Corp.*, cmt. #00395, at 17.

that the affirmative express consent standard would encourage vague disclosures at the outset to avoid the requirement for obtaining such consent.[281]

The Commission reaffirms its commitment to requiring companies to give prominent disclosures and to obtain express affirmative consent for material retroactive changes. Indeed, the Commission recently confirmed this approach in its settlements with Google and Facebook. The settlement agreements mandate that the companies give their users clear and prominent notice and obtain affirmative express consent prior to making certain material retroactive changes to their privacy practices.[282]

In response to the request for clarification on what constitutes a material change, the Commission notes that, at a minimum, sharing consumer information with third parties after committing at the time of collection not to share the data would constitute a material change. There may be other circumstances in which a change would be material, which would have to be determined on a case-by-case basis, analyzing the context of the consumer's interaction with the business.

The Commission further notes that commenters' concerns that the affirmative express consent requirement would encourage vague disclosures at the outset should be addressed by other elements of the framework. For example, other elements of the framework call on companies to improve and standardize their privacy statements so that consumers can easily glean and compare information about various companies' data practices. The framework also calls on companies to give consumers specific information and choice at a time and in a context that is meaningful to consumers. These elements, taken together, are intended to result in disclosures that are specific enough to be meaningful to consumers.

The preliminary staff report posed a question about the appropriate level of consent for prospective changes to companies' data collection and use. One commenter cited the rollout of Twitter's new user interface – "new Twitter" – as a positive example of a set of prospective changes about which consumers received ample and adequate notice and ability to exercise choice.[283] When "new Twitter" was introduced, consumers were given the opportunity to switch to or try out the new interface, or to keep their traditional Twitter profile. The Commission supports innovative efforts such as these to provide consumers with meaningful choices when a company proposes to change its privacy practices on a prospective basis.

(ii) Companies Should Obtain Consumers' Affirmative Express Consent Before Collecting Sensitive Data.

A variety of commenters discussed how to delineate which types of data should be considered sensitive. These comments reflect a general consensus that information about children, financial and health information, Social Security numbers, and precise, individualized geolocation data is sensitive and

281 *Comment of Facebook, Inc.*, cmt. #00413, at 10.

282 *See In the Matter of Google Inc.*, FTC Docket No. C-4336 (Oct. 13, 2011) (consent order), *available at* http://www.ftc.gov/os/caselist/1023136/111024googlebuzzdo.pdf; *In the Matter of Facebook, Inc.*, FTC File No. 092-3184 (Nov. 29, 2011) (proposed consent order), *available at* http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

283 *Comment of Electronic Frontier Foundation*, cmt. #00400, at 15.

merits heightened consent methods.[284] In addition, some commenters suggested that information related to race, religious beliefs, ethnicity, or sexual orientation, as well as biometric and genetic data, constitute sensitive data.[285] One commenter also characterized as sensitive information about consumers' online communications or reading and viewing habits.[286] Other commenters, however, noted the inherent subjectivity of the question and one raised concerns about the effects on market research if the definition of sensitive data is construed too broadly.[287]

Several commenters focused on the collection and use of information from teens, an audience that may be particularly vulnerable. A diverse coalition of consumer advocates and others supported heightened protections for teens between the ages of 13 and 17.[288] These commenters noted that while teens are heavy Internet users, they often fail to comprehend the long-term consequences of sharing their personal data. In order to better protect this audience, the commenters suggested, for example, limiting the amount of data that websites aimed at teens can collect or restricting the ability of teens to share their data widely through social media services.

Conversely, a number of industry representatives and privacy advocates objected to the establishment of different rules for teens.[289] These commenters cited the practical difficulties of age verification and the potential that content providers will simply elect to bar teen audiences.[290] Rather than requiring different choice mechanisms for this group, one company encouraged the FTC to explore educational efforts to address issues that are unique to teens.[291]

Given the general consensus regarding information about children, financial and health information, Social Security numbers, and precise geolocation data, the Commission agrees that these categories of information are sensitive. Accordingly, before collecting such data, companies should first obtain affirmative express consent from consumers. As explained above, the Commission also believes that companies should

284 *See*, *e.g., Comment of Consumer Federation of America*, cmt. #00358, at 9; *Comment of CNIL*, cmt. #00298, at 4; *Comment of Massachusetts Office of the Attorney General*, cmt. #00429, at 3; *Comment of Kindsight*, cmt. #00344, at 11; *Comment of Experian*, cmt. #00398, at 9; *Comment of Center for Democracy & Technology,* cmt. #00469, at 14; *Comment of Office of the Information and Privacy Commissioner of Ontario,* cmt. #00239, at 2; *see also Comment of TRUSTe,* cmt. #00450, at 11 (agreeing that sensitive information should be defined to include information about children, financial and medical information, and precise geolocation information but urging that sensitive information be more broadly defined as "information whose unauthorized disclosure or use can cause financial, physical, or reputational harm"); *Comment of Facebook, Inc.*, cmt. #00413, at 23 (agreeing that sensitive information may warrant enhanced consent, but noting that enhanced consent may not be possible for activities such as the posting of status updates by users where those updates may include sensitive information such as references to an illness or medical condition).

285 *See Comment of Consumer Federation of America*, cmt. #00358, at 9; *see also Comment of CNIL*, cmt. #00298, at 4, *Comment of Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 35.

286 *See Comment of Electronic Frontier Foundation*, cmt. #00400, at 7.

287 *See Comment of Marketing Research Ass'n*, cmt. #00405, at 6-7; *Comment of American Trucking Ass'ns*, cmt. #00368, at 2-3; *Comment of Microsoft Corp.*, cmt. #00395, at 10.

288 *See Comment of Institute for Public Representation*, cmt. #00346, at 4; *Comment of Consumers Union*, cmt. #00362, at 13.

289 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 15; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 12-13; *Comment of Microsoft Corp.*, cmt. #00395, at 10; *see also Comment of Electronic Frontier Foundation*, cmt. #00400, at 14 (opposing the creation of special rules giving parents access to data collected about their teenaged children); *Comment of PrivacyActivism*, cmt. #00407, at 4 (opposing the creation of special rules giving parents access to data collected about their teenaged children).

290 *See Comment of Center for Democracy & Technology*, cmt. #00469, at 15; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 12-13; *Comment of Microsoft Corp.*, cmt. #00395, at 10.

291 *See Comment of Microsoft Corp.*, cmt. #00395, at 10.

follow this practice irrespective of whether they use the sensitive data for first-party marketing or share it with third parties.[292]

The Commission is cognizant, however, that whether a particular piece of data is sensitive may lie in the "eye of the beholder" and may depend upon a number of subjective considerations. In order to minimize the potential of collecting any data – whether generally recognized as sensitive or not – in ways that consumers do not want, companies should implement *all* of the framework's components. In particular, a consumer's ability to access – and in appropriate cases to correct or delete – data will allow the consumer to protect herself when she believes the data is sensitive but others may disagree.

With respect to whether information about teens is sensitive, despite the difficulties of age verification and other concerns cited in the comments, the Commission agrees that companies that target teens should consider additional protections. Although affirmative express consent may not be necessary in every advertising campaign directed to teens, other protections may be appropriate. For example, all companies should consider shorter retention periods for teens' data.

In addition, the Commission believes that social networking sites should consider implementing more privacy-protective default settings for teens. While some teens may circumvent these protections, they can function as an effective "speed bump" for this audience and, at the same time, provide an opportunity to better educate teens about the consequences of sharing their personal information. The Commission also supports access and deletion rights for teens, as discussed below.[293]

Final Principle: For practices requiring choice, companies should offer the choice at a time and in a context in which the consumer is making a decision about his or her data. Companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes.

D. TRANSPARENCY

Baseline Principle: Companies should increase the transparency of their data practices.

Citing consumers' lack of awareness of how, and for what purposes, companies collect, use, and share data, the preliminary staff report called on companies to improve the transparency of their data practices. Commission staff outlined a number of measures to achieve this goal. One key proposal, discussed in the previous section, is to present choices to consumers in a prominent, relevant, and easily accessible place at a time and in a context when it matters to them. In addition, Commission staff called on industry to make privacy statements clearer, shorter, and more standardized; give consumers reasonable access to their data; and undertake consumer education efforts to improve consumers' understanding of how companies collect, use, and share their data.

292 *See infra* at Section IV.C.1.b.(v).

293 *See infra* at Section IV.D.2.b.

Commenters offered proposals for how to achieve greater transparency and sought clarification on how they should implement these elements of the framework. Although the Commission adopts the proposed framework's transparency principle without change, it clarifies the application of the framework in response to these comments, as discussed below.

1. PRIVACY NOTICES

Proposed Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

The preliminary staff report highlighted the consensus among roundtable participants that most privacy policies are generally ineffective for informing consumers about a company's data practices because they are too long, are difficult to comprehend, and lack uniformity.[294] While acknowledging privacy policies' current deficiencies, many roundtable participants agreed that the policies still have value – they provide an important accountability function by educating consumer advocates, regulators, the media, and other interested parties about the companies' data practices.[295] Accordingly, Commission staff called on companies to provide clear and concise descriptions of their data collection and use practices. Staff further called on companies to standardize the format and the terminology used in privacy statements so that consumers can compare the data practices of different companies and exercise choices based on privacy concerns, thereby encouraging companies to compete on privacy.

Despite the consensus from the roundtables that privacy statements are not effective at communicating a company's data collection and use practices to consumers, one commenter disagreed that privacy notices need to be improved.[296] Another commenter pointed out that providing more granular information about data collection and use practices could actually increase consumer confusion by overloading the consumer with information.[297] Other industry commenters highlighted the work they have undertaken since the preliminary staff report to improve their own privacy statements.[298]

Many consumer groups supported staff's call to standardize the format and terminology used in privacy statements so that consumers could more easily compare the practices of different companies.[299] Some commenters suggested a "nutrition label" approach for standardizing the format of privacy policies and cited

294 Recent research and surveys suggests that many consumers (particularly among lower income brackets and education levels) do not read or understand privacy policies, thus further heightening the need to make them more comprehensible. Notably, in a survey conducted by Zogby International, 93% of adults – and 81% of teens – indicated they would take more time to read terms and conditions for websites if they were shorter and written in clearer language. *See Comment of Common Sense Media*, cmt. #00457, at 1.

295 *See Comment of AT&T , Inc.*, cmt. #00420, at 17; *Comment of Center for Democracy & Technology*, cmt. #00469, at 24.

296 *See Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 22.

297 *See Comment of United States Council for International Business*, cmt. #00366, at 3.

298 *See Comment of Google Inc.*, cmt. #00417, at 1; *Comment of Facebook, Inc.*, cmt. #00413, at 9; *Comment of AT&T Inc.*, cmt. #00420, at 24.

299 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 15-16; *Comment of Consumer Federation of America*, cmt. #00358, at 16; *Comment of Consumer Watchdog*, cmt. #00402, at 2.

research underway in this area.[300] Another suggested the "form builder" approach used for GLBA Short Notices to standardize the format of privacy notices outside the financial context.[301] One consumer group called for standardization of specific terms like "affiliate" and "anonymize" so that companies' descriptions of their data practices are more meaningful.[302] A wide range of commenters suggested that different industry sectors come together to develop standard privacy notices.[303] Other commenters opposed the idea of mandated standardized notices, arguing that the Commission should require only that privacy statements be clear and in plain language. These commenters stated that privacy statements need to take into account differences among business models and industry sectors.[304]

Privacy statements should account for variations in business models across different industry sectors, and prescribing a rigid format for use across all sectors is not appropriate. Nevertheless, the Commission believes that privacy statements should contain some standardized elements, such as format and terminology, to allow consumers to compare the privacy practices of different companies and to encourage companies to compete on privacy. Accordingly, Commission calls on industry sectors to come together to develop standard formats and terminology for privacy statements applicable to their particular industries. The Department of Commerce will convene multi-stakeholder groups to work on privacy issues; this could be a useful venue in which industry sectors could begin the exercise of developing more standardized, streamlined privacy policies.

Machine-readable policies,[305] icons, and other alternative forms of providing notice also show promise as tools to give consumers the ability to compare privacy practices among different companies.[306] In response to the preliminary staff report's question on machine-readable policies, commenters agreed that such policies could improve transparency.[307] One commenter proposed combining the use of machine-readable policies with icons and standardized policy statements (*e.g.*, "we collect but do not share consumer data

300 *See Comment of Consumer Watchdog*, cmt. #00402, at 2; *Comment of Consumer Federation of America*, cmt. #00358, at 16; *see also Comment of Lorrie Faith Cranor*, cmt. #00453, at 2 n.7 (discussing P3P authorizing tools that enable automatic generation of "nutrition label" privacy notices).

301 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 16.

302 *See Comment of Electronic Frontier Foundation*, cmt. #00400, at 6.

303 *See Comment of General Electric*, cmt. #00392, at 2; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 4; *Comment of Consumers Union*, cmt. #00362, at 15-16; *Comment of Facebook, Inc.*, cmt. #00413, at 9.

304 *See Comment of AT&T Inc.*, cmt. #00420, at 25; *Comment of eBay*, cmt. #00374, at 10; *Comment of National Cable & Telecommunications Ass'n*, cmt. #00432, at 29; *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at 12; *Comment of Microsoft Corp.*, cmt. #00395, at 15.

305 A machine-readable privacy policy is a statement about a website's privacy practices – such as the collection and use of data – written in a standard computer language (not English text) that software tools such as consumer's web browser can read automatically. For example, when the browser reads a machine-readable policy, the browser can compare the policy to the consumer's browser privacy preferences, and can inform the consumer when these preferences do not match the practices of the website he is visiting. If the consumer decides he does not want to visit websites that sell information to third parties, he might set up a rule that recognizes that policy and blocks such sites or display a warning upon visiting such a site. Machine-readable language will be the subject of an upcoming summit. *See* White House, National Archives & Records Administration, *Informing Consumers Through Smart Disclosures* (Mar. 1, 2012), *available at* http://www.nist.gov/ineap/upload/Summit_Invitation_to_Agencies_FINAL.pdf (describing upcoming summit).

306 Likewise, new tools like privacyscore.com may help consumers more readily compare websites' data practices. *See* Tanzina Vega, *A New Tool in Protecting Online Privacy*, N.Y. Times, Feb. 12, 2012, *available at* http://mediadecoder.blogs.nytimes.com/2012/02/12/a-new-tool-in-protecting-online-privacy/?scp=2&sq=privacy&st=cse.

307 *Comment of Phorm Inc.*, cmt. #00353, at 9; *Comment of Lorrie Faith Cranor*, cmt. #00453, at 6.

with third parties") to simplify privacy decision-making for consumers.[308] Other commenters described how icons work or might work in different business contexts. One browser company described efforts underway to develop icons that might be used to convey information, such as whether a consumer's data is sold or may be subject to secondary uses, in a variety of business contexts.[309] Representatives from online behavioral advertising industry groups also described their steps in developing and implementing an icon to communicate that online behavioral advertising may be taking place.[310]

Commenters also discussed the particular challenges associated with providing notice in the mobile context, noting the value of icons, summaries, FAQs, and videos.[311] Indeed, some work already has been done in this area to increase the transparency of data practices. For example, the advocacy organization Common Sense Media reviews and rates mobile apps based on a variety of factors including privacy[312] and a platform provider uses an icon to signal to consumers when a mobile application is using location information.[313] In addition, CTIA – a wireless industry trade group – in conjunction with the Entertainment Software Rating Board, recently announced plans to release a new rating system for mobile apps.[314] This rating system, which is based on the video game industry's model, will use icons to indicate whether specific apps are appropriate for "all ages," "teen," or only "adult" audiences. The icons will also detail whether the app shares consumers' personal information. Noting the complexity of the mobile ecosystem, which includes device manufacturers, operating system providers, mobile application developers, and wireless carriers, some commenters called for public workshops to bring together different stakeholders to develop a uniform approach to icons and other methods of providing notice.[315] Also, as noted above, the Mobile Marketing Association has released its Mobile Application Privacy Policy.[316]

The Commission appreciates the complexities of the mobile environment, given the multitude of different entities that want to collect and use consumer data and the small space available for disclosures

308 *Comment of Lorrie Faith Cranor*, cmt. #00453, at 6 (explaining how icons combined with standard policies might work: "For example, a type I policy might commit to not collecting sensitive categories of information and not sharing personal data except with a company's agents, while a type II policy might allow collection of sensitive information but still commit to not sharing them, a type III policy might share non-identified information for behavioral advertising, and so on. Companies would choose which policy type to commit to. They could advertise their policy type with an associated standard icon, while also providing a more detailed policy. Users would be able to quickly determine the policy for the companies they interact with.").

309 *Comment of Mozilla*, cmt. #00480, at 12.

310 *Comment of American Ass'n of Advertising Agencies, American Advertising Federation, Ass'n of National Advertisers, Direct Marketing Ass'n, Inc., and Interactive Advertising Bureau*, cmt. #00410 at 2-3; *Comment of Digital Marketing Alliance*, cmt. #00449, at 18-24; *Comment of Evidon*, cmt. #00391, at 3-6; *Comment of Internet Advertising Bureau*, cmt. #00388, at 4.

311 *Comment of General Electric*, cmt. #00392, at 1-2; *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 2-3; *Comment of Mozilla*, cmt. #00480, at 12.

312 *See* Common Sense Media, App Reviews, http://www.commonsensemedia.org/app-reviews.

313 *See* Letter from Bruce Sewell, General Counsel & Senior Vice President of Legal and Governmental Affairs, Apple, to Hon. Edward J. Markey, U.S. House of Representatives (May 6, 2011), *available at* http://robert.accettura.com/wp-content/uploads/2011/05/apple_letter_to_ejm_05.06.11.pdf.

314 *See* Press Release, CTIA – The Wireless Ass'n, CTIA – The Wireless Ass'n to Announce Mobile Application Rating System with ESRB (Nov. 21, 2011), *available at* http://www.ctia.org/media/press/body.cfm/prid/2145.

315 *Comment of Consumer Federation of America*, cmt. #00358, at 16; *Comment of GSMA*, cmt. #00336, at 10.

316 Although this effort is promising, more work remains. The Mobile Marketing Association's guidelines are not mandatory and there is little recourse against companies who elect not to follow them. More generally, there are too few players in the mobile ecosystem who are committed to self-regulatory principles and providing meaningful disclosures and choices.

on mobile screens. These factors increase the urgency for the companies providing mobile services to come together and develop standard notices, icons, and other means that the range of businesses can use to communicate with consumers in a consistent and clear way.

To address this issue, the Commission notes that it is currently engaged in a project to update its existing business guidance about online advertising disclosures.[317] In conjunction with this project, Commission staff will host a workshop later this year.[318] One of the topics to be addressed is mobile privacy disclosures: How can these disclosures be short, effective, and accessible to consumers on small screens? The Commission hopes that the discussions at the workshop will spur further industry self-regulation in this area.

Final Principle: Privacy notices should be clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices.

2. ACCESS

Proposed Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

There was broad agreement among a range of commenters that consumers should have some form of access to their data. Many of these commenters called for flexibility, however, and requested that access rights be tiered according to the sensitivity and intended use of the data at issue.[319] One commenter argued that access rights should be limited to sensitive data, such as financial account information, because a broader access right would be too costly for offline retailers.[320] Some companies and industry representatives supported providing consumers full access to data that is used to deny benefits; several commenters affirmed the significance of the FCRA in providing access to information used for critical decisionmaking. For other less sensitive data, such as marketing data, they supported giving consumers a general notice describing the types of data they collect and the ability to suppress use of the data for future marketing.[321]

One commenter raised concerns about granting access and correction rights to data files used to prevent fraudulent activity, noting that such rights would create risks of fraud and identity theft. This commenter also stated that companies would need to add sensitive identifying information to their marketing databases in order to authenticate a consumer's request for information, and that the integration of multiple databases would raise additional privacy and security risks.[322]

317 *See* Press Release, FTC, FTC Seeks Input to Revising its Guidance to Business About Disclosures in Online Advertising (May 26, 2011), *available at* http://www.ftc.gov/opa/2011/05/dotcom.shtm.

318 *See* Press Release, FTC, FTC Will Host Public Workshop to Explore Advertising Disclosures in Online and Mobile Media on May 30, 2012 (Feb. 29, 2012), *available at* http://www.ftc.gov/opa/2012/02/dotcom.shtm.

319 *Comment of Intuit, Inc.*, cmt. #00348, at 12; *Comment of eBay*, cmt. #00374, at 10; *Comment of IBM*, cmt. #00433, at 3; *Comment of Consumers Union*, cmt. #00362, at 16.

320 *Comment of Meijer*, cmt. #00416, at 7.

321 *Comment of Intel Corp.*, cmt. #00246, at 8; *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 8; *Comment of Experian*, cmt. #00398, at 11.

322 *Comment of Experian*, cmt. #00398, at 10-11.

A number of commenters raised issues about the costs associated with providing access. One company suggested that access rights be flexible, taking into account the company's existing data infrastructure.[323] Others argued that access be granted only to consumer information that is "reasonably accessible in the course of business"[324] and one commenter said that companies should be able to charge for providing access where there are costs associated with retrieving and presenting data.[325]

Commenters also asserted that companies should tell consumers the entities with which their data has been shared.[326] Citing California's "Shine the Light" law, one commenter stated that companies should not only identify the third parties with which they share consumer data but should also disclose how the third parties use the data for marketing.[327] Another commenter pointed out that many marketers do not maintain records about data sold to other companies on an individual basis. Thus, marketers have the ability to identify the companies to which they have sold consumer data in general, but not the third parties with which they may have shared the information about any individual consumer.[328]

Some comments reflect support for requiring companies to identify for consumers the sources of data collected about them so that consumers can correct erroneous data at the source, if appropriate.[329] One commenter noted that the DMA self-regulatory guidelines currently require that a marketer identify the sources of data maintained about consumers.[330]

The Commission agrees with the commenters who stated that consumer access should be proportional to the sensitivity and the intended use of the data at issue. Indeed, the comments generally support treating access in accordance with three categories that reflect different levels of data sensitivity: (1) entities that maintain data for marketing purposes; (2) entities subject to the FCRA; and (3) entities that may maintain data for other, non-marketing purposes that fall outside of the FCRA.

At one side of the spectrum are companies that maintain data for marketing purposes. For data used solely for marketing purposes, the Commission agrees with the commenters who stated that the costs of providing individualized access and correction rights would likely outweigh the benefits. The Commission continues to support the idea of businesses providing consumers with access to a list of the categories of consumer data they hold, and the ability to suppress the use of such data for marketing. This approach

323 *Comment of AT&T Inc.,* cmt. #00420, at 28-29.

324 *Comment of CTIA - The Wireless Ass'n*, cmt. #00375, at 3; *Comment of Yahoo!, Inc.*, cmt. #00444, at 20; *Comment of The Centre for Information Policy Leadership at Hunton & Williams LLP*, cmt. #00360, at 5-6.

325 *Comment of U.S. Council for International Business*, cmt. #00366, at 3.

326 *Comment of Catalog Choice*, cmt. #00473, at 8-9; *Comment of the Information Commissioner's Office of the UK*, cmt. #00249, at 5.

327 *See Comment of Catalog Choice*, cmt. #00473, at 20. Under this law, businesses, upon request, must provide their customers, free of charge and within 30 days: (1) a list of the categories of personal information disclosed by the business to third parties for the third parties' marketing purposes, (2) the names and addresses of all of the third parties that received personal information from the business in the preceding calendar year, (3) and if the nature of the third parties's business cannot reasonably be determined from the third parties' name, examples of the products or services marketed by the third party. Cal. Civ. Code § 1798.83.

328 *Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7.

329 *Comment of Reputation.com, Inc.*, cmt. #00385, at 11-12; *see also Comment of Center for Democracy & Technology*, cmt. #00469, at 25.

330 *Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7.

will provide consumers with an important transparency tool without imposing significant new costs for businesses.[331]

The Commission does, however, encourage companies that maintain consumer data for marketing purposes to provide more individualized access when feasible. One example of an innovation in this area is the advertising preference managers that companies such as Google and Yahoo! have implemented. Yahoo!, for example, offers consumers, through its Ad Interest Manager, the ability to access the specific interest categories that Yahoo! associates with individual consumers and allows them to suppress marketing based on some or all of these categories. Using this service, an elementary school teacher who conducted online research for pet food during the time she owned a dog, but continues to receive advertisements for dog food, could remove herself from the "Consumer Packaged Goods > Pets and Animals > Food and Supplies" category while still opting to remain part of the "Life Stages > Education > K to 12" category.[332] The Commission supports efforts by companies to provide consumers with these types of granular choices to give them greater control over the marketing materials and solicitations they receive.

At the other end of the spectrum are companies that assemble and evaluate consumer information for use by creditors, employers, insurance companies, landlords, and other entities involved in eligibility decisions affecting consumers. The preliminary staff report cited the FCRA as an important tool that provides consumers with the right to access their own data that has been used to make such decisions, and if it is erroneous, to correct it. Several commenters echoed this view.[333]

The FCRA recognizes the sensitivity of the data that consumer reporting agencies maintain and the ways in which various entities use it to evaluate whether a consumer is able to participate in so many activities central to modern life; therefore, it provides consumers with access and correction rights for information contained in consumer reports. Pursuant to the FCRA, consumer reporting agencies are required to disclose to consumers, upon request, all items in the consumer's file, no matter how or where they are stored, as well as the entities with which the consumer reporting agency shared the information in a consumer's report. When consumers identify information in their report that is incomplete or inaccurate, and report it to a consumer reporting agency, the agency must investigate and correct or delete such information in certain circumstances.

As more and more consumer data becomes available from a variety of sources, companies are increasingly finding new opportunities to compile, package, and sell that information. In some instances, companies could be compiling and selling this data to those who are making decisions about a consumer's eligibility for credit, insurance, employment, and the like. To the extent companies are assembling data and marketing or selling it for such purposes, they are subject to the FCRA. For example, companies that compile social media information and provide it to employers for use in making hiring decisions are consumer reporting

331 As discussed above, in most cases the framework does not require companies to provide consumer choice for first-party marketing, although first parties may choose to provide such choice to meet consumer demand. Outside of the first-party marketing context, however, companies should provide consumers with the ability to suppress the use of their data for marketing.

332 *See* Yahoo!, Ad Interest Manager, http://info.yahoo.com/privacy/us/yahoo/opt_out/targeting.

333 *Comment of Consumer Data Industry Ass'n*, cmt. #00363, at 4 - 5; *Comment of Experian*, cmt. #00398, at 10.

agencies and thus required to provide consumers with access and correction rights under the FCRA.[334] These companies would also be required to inform employers about their FCRA obligation to provide adverse action notices when, for example, employment is denied.

Even if a company is not compiling and sharing data for the specific purpose of making employment, credit, or insurance eligibility decisions, if the company has reason to believe the data will be used for such purposes, it would still be covered by the FCRA. For example, recently, the Commission issued warning letters to the developers of mobile apps that compiled public record information on individuals and created apps for the purposes of learning information about friends, co-workers, neighbors, or potential suitors.[335] The Commission noted that if these apps marketed their services for employment purposes or otherwise had reason to believe that they were being used for employment purposes, the FCRA requirements would apply.

Finally, some businesses may maintain and use consumer data for purposes that do not fall neatly within either the FCRA or marketing categories discussed above. These businesses may encompass a diverse range of industry sectors. They may include businesses selling fraud prevention or risk management services, in order to verify the identities of customers. They may also include general search engines, media publications, or social networking sites. They may include debt collectors trying to collect a debt. They may also include companies collecting data about how likely a consumer is to take his or her medication, for use by health care providers in developing treatment plans.[336]

For these entities, the Commission supports the sliding scale approach, which several commenters endorsed,[337] with the consumer's ability to access his or her own data scaled to the use and sensitivity of the data. At a minimum, these entities should offer consumers access to (1) the types of information the companies maintain about them;[338] and (2) the sources of such information.[339] The Commission believes that requiring companies to identify data sources would help consumers to correct erroneous information at the source. In appropriate circumstances the Commission urges companies to provide the names of the third parties with whom consumer information is shared.

In instances where data is more sensitive or may affect benefits, more individualized notice, access, and correction rights may be warranted. For example, if a company denies services to a consumer because it could not verify the consumer's identity, it may be appropriate for the company to disclose the name of the identity verification service used. This will allow the consumer to contact the data source, which can then provide the consumer with access to the underlying information, as well as any appropriate remedies, such

334 15 U.S.C. §§ 1681g-1681h. *See* Letter from Maneesha Mithal, Assoc. Dir., Div. of Privacy and Identity Prot., FTC, to Renee Jackson, Counsel for Social Intelligence Corp., (May 9, 2011) (closing letter), *available at* http://www.ftc.gov/os/closings/110509socialintelligenceletter.pdf .

335 *See* Press Release, FTC, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting Act (Feb. 7, 2012), *available at* http://www.ftc.gov/opa/2012/02/mobileapps.shtm (describing warning letters sent by the FTC to Everify, Inc., InfoPay, Inc., and Intelligator, Inc. on Jan. 25, 2012).

336 *See* Laura Landro, *Many Pills, Many Not Taken*, Wall St. J., Oct. 10, 2011, *available at* http://online.wsj.com/article/SB10001424052970203388804576616882856318782.html.

337 *Comment of Consumers Union*, cmt. #00362, at 16; *Comment of CTIA – The Wireless Ass'n*, cmt. #00375, at 7; *Comment of Microsoft Corp.*, cmt. #00395, at 15-16.

338 *Comment of Retail Industry Leaders Ass'n*, cmt. #00352, at Ex. A.

339 *Comment of Reputation.com, Inc.*, cmt. #00385, at 11-12. Of course, First Amendment protections would apply to journalists' sources, among other things, and the Commission's recommendations are not intended to apply in that area.

as the ability to correct the information.[340] To ensure that the consumer knows that she has been denied a benefit based on her own data, as a best practice the company should notify the consumer of the denial and the information on which the denial was based.

Verifying the identity of users who seek access to their own information is an important consideration and should be approached from a risk management perspective, focusing on the likelihood of and potential harm from misidentification. Indeed, in the example of identity verification services described above, one would not want a criminal to be able to "correct" his or her own truthful data, and it would be appropriate to require somewhat more stringent safeguards and proof of identity before allowing access and correction. Certainly, consumer reporting agencies have developed procedures allowing them to verify the identity of requesting consumers using the multiple pieces of information they have about consumers to match information provided by the requesting consumer. Companies engaged in providing data for making eligibility determinations should develop best practices for authenticating consumers for access purposes.

On the other hand, the significantly reduced risks associated with providing the wrong person's information contained in a marketing database that contains no sensitive information may justify less stringent authentication procedures.[341] As with other issues discussed in this Report, reasonableness should be the touchstone: the degree of authentication employed should be tied to the sensitivity of the information maintained and how such information is used.

a. Special Access Mechanism for Data Brokers

Data brokers are companies that collect information, including personal information about consumers, from a wide variety of sources for the purpose of reselling such information to their customers for various purposes, including verifying an individual's identity, differentiating records, marketing products, and preventing financial fraud. Several commenters noted the lack of transparency about the practices of these entities, which often have a wealth of information about consumers but never interact directly with them.[342] Consumers are often unaware of the existence of these entities, as well as the purposes for which they collect and use data.[343] One commenter noted that data brokers may sell data to employers, background screeners, and law enforcement, among others, without the consumer's knowledge.[344] The Commission has monitored data brokers since the 1990s, hosting workshops, drafting reports, and testifying before Congress about

340 As noted above, companies should pay close attention to the types of eligibility determinations being made to ensure they comply with the FCRA, if warranted.

341 One commenter noted that when organizations collect and maintain sensitive information about individuals, such as for banking or issuance of credit, they will ask for authenticating information before an individual can access those records. This same commenter then stated that organizations holding less sensitive data may not require similarly rigorous authentication. *See Comment of The Centre for Information Policy Leadership at Hunton & Williams, LLP*, cmt. #00360, at 7 n.6.

342 *See Comment of Privacy Rights Clearinghouse*, cmt. #00351, at 3; *Comment of Consumers Union*, cmt. #00362, at 11.

343 *See Comment of Consumer Federation of America*, cmt. #00358, at 17.

344 *See Comment of Privacy Rights Clearinghouse,* cmt. #00351, at 8.

the privacy implications of data brokers' practices.[345] Following a Commission workshop, the data broker industry created the Individual References Services Group (IRSG), a self-regulatory organization for certain data brokers.[346] Although industry ultimately terminated this organization, a series of public breaches – including one involving ChoicePoint – led to renewed scrutiny of the practices of data brokers.[347] And, indeed, there have been few broad-based efforts to implement self-regulation in this area in the recent past.

The access rights discussed above will help to improve the transparency of companies' data practices generally, whether or not they have a direct consumer interface. Because most data brokers are invisible to consumers, however, the Commission makes two additional recommendations as to these entities.

First, since 2009, the Commission has supported legislation giving access rights to consumers for information held by data brokers. During the 111th Congress, the House approved a bill that included provisions to establish a procedure for consumers to access information held by data brokers.[348] To improve the transparency of this industry's practices, the Commission has testified in support of the goals of this legislation[349] and continues to support legislation in this area.[350]

Second, the Commission recommends that the data broker industry explore the idea of creating a centralized website where data brokers that compile and sell data for marketing could identify themselves to consumers and describe how they collect consumer data and disclose the types of companies to which they sell the information. Additionally, data brokers could use the website to explain the access rights and other choices they offer consumers, and could offer links to their own sites where consumers could exercise such options.[351] This website will improve transparency and give consumers control over the data practices of companies that maintain and share data about them for marketing purposes. It can also provide consumer-facing entities such as retailers a means for ensuring that the information brokers from which they purchase "enhancement" information have instituted appropriate transparency and control mechanisms. Indeed, the

345 *See, e.g.*, Prepared Statement of the FTC, *Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information*: *Hearing Before the Senate Comm. on Banking, Housing, and Urban Affairs,* 109th Cong. (Mar. 10, 2005), *available at* http://www.ftc.gov/os/testimony/050310idtheft.pdf; *see also* FTC Workshop, *The Information Marketplace: Merging & Exchanging Consumer Data* (Mar. 13, 2001), *available at* http://www.ftc.gov/bcp/workshops/infomktplace/index.shtml; FTC Workshop, *Information Flows: The Costs and Benefits to Consumers and Businesses of the Collection and Use of Consumer Information* (June 18, 2003), *available at* http://www.ftc.gov/bcp/workshops/infoflows/030618agenda.shtm.

346 *See* FTC, *Individual Reference Services, A Report to Congress* (1997), *available at* http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm.

347 *See* Prepared Statement of the FTC, *Protecting Consumers' Data: Policy Issues Raised by ChoicePoint*: *Hearing before H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection, Comm. on Energy and Commerce*, 109th Cong. (Mar. 15, 2005), *available at* http://www.ftc.gov/os/2005/03/050315protectingconsumerdata.pdf.

348 Data Accountability and Trust Act, H.R. 2221, 111th Congress (as passed by House, Dec. 8, 2009).

349 *See, e.g.,* Prepared Statement of the FTC, *Legislative Hearing on H.R. 2221, the Data Accountability and Protection Act, and H.R. 1319, the Informed P2P User Act: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Trade, and Consumer Protection*, 111th Cong. (May 5, 2009), *available at* http://www.ftc.gov/os/2009/05/P064504peertopeertestimony.pdf.

350 *See, e.g.,* Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong. (May 4, 2011), *available at* http://www.ftc.gov/opa/2011/05/pdf/110504datasecurityhouse.pdf; Prepared Statement of the FTC, *Data Security: Hearing Before the H. Comm. on Energy and Commerce, Subcomm. on Commerce, Manufacturing, and Trade*, 112th Cong.(June 15, 2011), *available at* http://www.ftc.gov/os/testimony/110615datasecurityhouse.pdf; Prepared Statement of the FTC, *Protecting Consumers in the Modern World: Hearing Before the S. Comm. on Commerce, Science, and Transportation*, 112th Cong. (June 29, 2011), *available at* http://www.ftc.gov/os/testimony/110629privacytestimonybrill.pdf.

351 *See Comment of World Privacy Forum*, cmt. #00376, at 6; *Comment of Consumer Federation of America*, cmt. #00358, at 17-18.

consumer-facing entities could provide consumers with a link to the centralized mechanism, after having made sure that the data brokers from which they buy data participate in such a system. The Commission will discuss with relevant industry members how this mechanism could be developed and implemented voluntarily, in order to increase the transparency of their data practices and give consumers tools to opt out.[352]

b. Access to Teen Data

One commenter proposed that teens be given regular access to whether and how their data has been shared because of their particular vulnerability to ubiquitous marketing messages and heavy use of social media and mobile devices.[353] Others noted that teens in particular may not appreciate the persistence and future effects of data that they post about themselves online and thus need a "right to be forgotten." In its comment, the French Data Protection authority advocated the "right to be forgotten," which would allow consumers to withdraw data posted online about themselves at any point, for all users, but noted in particular the need to have control over information posted in one's youth.[354] In the United States, legislation has been introduced that would give teens an eraser button, which would allow them to erase certain material on social networking sites.[355]

The Commission generally supports exploration of the idea of an "eraser button," through which people can delete content that they post online. Many companies already offer this type of feature,[356] which is consistent with the principles of data access and suppression. Such an "eraser button" could be particularly useful for teens who might not appreciate the long-term consequences of their data sharing. Teens tend to be more impulsive than adults[357] and, as a result, may voluntarily disclose more information online than they should, leaving them vulnerable to identity theft or adversely affecting potential employment or college admissions opportunities. In supporting an eraser button concept, the Commission notes that such a feature

352 The current website of the Direct Marketing Association (DMA) offers an instructive model for such a mechanism. The DMA – which consists of data brokers, retailers, and others – currently offers a service through which consumers can opt out of receiving marketing solicitations via particular channels, such as direct mail, from DMA member companies. *See* DMAChoice, http://www.dmachoice.org/dma/member/home.action.

353 *See Comment of Consumers Union*, cmt. #00362, at 13; *see also Center for Digital Democracy and U.S. PIRG*, cmt. #00338, at 39.

354 *Comment of CNIL*, cmt. #00298, at 3.

355 Do Not Track Kids Act of 2011, H.R. 1895, 112th Congress (2011).

356 *See* Facebook, How Do I Remove a Wall Post or Story?, *available at* http://www.facebook.com/help/?page=174851209237562; LinkedIn, Privacy Policy, http://www.linkedin.com/static?key=privacy_policy.

357 *See, e.g.,* FTC, *Transcript of March 17, 2010, Privacy Roundtable, Panel 3: Addressing Sensitive Information*, 208-215, *available at* http://www.ftc.gov/bcp/workshops/privacyrountables/PrivacyRoundtable_March2010_Transcript.pdf; *see also* Chris Hoofnagle, Jennifer King, Su Li, & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?* (Apr. 14, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864.

would have to be carefully crafted in order to avoid implicating First Amendment concerns.[358] It would also need to be technically feasible and proportional to the nature, sensitivity, and amount of data collected.

Final Principle: Companies should provide reasonable access to the consumer data they maintain; the extent of access should be proportionate to the sensitivity of the data and the nature of its use.

3. CONSUMER EDUCATION

Proposed Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

In its preliminary report, FTC staff called for all stakeholders to accelerate their efforts to raise consumer awareness about data practices and to provide additional transparency tools to consumers. Staff pointed out that consumers need more education about the privacy implications of various data practices so that they can make informed decisions about the trade-offs involved. Staff posed questions about how the range of interested stakeholders – companies, industry associations, consumer groups, and government – can do a better job of informing consumers about privacy. Many commenters expressed general support for the notion that consumer education is a vital component of improving privacy protections for consumers.[359] One commenter suggested that businesses use their creative talents to make privacy more accessible for consumers, and as support, pointed to its own privacy game.[360] The game teaches players about privacy by inviting them to tour a virtual small town in which the buildings represent different parts of the commenter's privacy policy.

Over the last few years, a number of other companies and industry and consumer groups have stepped up their efforts to educate consumers about privacy and their privacy choices.[361] The Commission encourages more such efforts, with an eye toward developing clear and accessible messages that consumers will see and understand.

358 While consumers should be able to delete much of the information they place on a particular social media site, there may be First Amendment constraints to requiring third parties to delete the same information. In the FTC's recent proposed settlement with Facebook, the company agreed to implement measures designed to prevent any third party from accessing information under Facebook's control within a reasonable time period, not to exceed thirty days, from the time the user has deleted such information. *See In the Matter of Facebook, Inc.,* FTC File No. 092 3184 (Nov. 29, 2011) (proposed consent order), *available at* http://ftc.gov/os/caselist/0923184/111129facebookagree.pdf.

359 *See, e.g., Comment of Intuit Inc.*, cmt. #00348, at 12; *Comment of AT&T Inc.*, cmt. #00420, at 30-31; *Comment of Consumers Union*, cmt. #00362, at 18.

360 *Comment of Zynga Inc.*, cmt. #00459, at 4.

361 *See, e.g.,* Common Sense Media, App Reviews, http://www.commonsensemedia.org/app-reviews (listing reviews that evaluate privacy and safety concerns posed by common mobile applications designed for children); Google, Ad Preferences, Frequently Asked Questions, http://www.google.com/ads/preferences/html/faq.html; Interactive Advertising Bureau, Privacy Matters Campaign, http://www.iab.net/privacymatters/campaign.php; Kashmir Hill, *Zynga's PrivacyVille – It's Not Fun, But It Gets the Job Done,* Forbes, July 8, 2011, *available at* http://www.forbes.com/sites/kashmirhill/2011/07/08/zyngas-privacyville-its-not-fun-but-it-gets-the-job-done/.

A range of commenters suggested that the FTC explicitly endorse or sponsor various private sector-led consumer education efforts.[362] The Commission certainly supports private sector education efforts, and encourages private sector entities to freely use the FTC's extensive consumer and business education materials, under their own branding.

For example, the FTC encourages businesses to use information from its OnGuardOnline.gov website, which aims to help people be safe, secure and responsible online. The OnGuardOnline.gov campaign is a partnership of 15 federal agencies. The site includes articles, videos, games and tutorials to teach home users, small businesses or corporate employees about privacy-related topics like using Wi-Fi networks, peer-to-peer file sharing, mobile apps, and online tracking. The OnGuard Online Blog provides the latest cybersecurity news and practical tips from the FTC and other federal agencies. The FTC publishes this blog regularly and encourages companies to copy and disseminate it. Additionally, the FTC has continued its own consumer education efforts in the privacy area. Over the last year, the Commission released consumer education materials on a variety of topics including: using Wi-Fi hot spots; managing browser and "Flash" cookies; understanding mobile privacy; and protecting against child identity theft.[363]

Final Principle: All stakeholders should expand their efforts to educate consumers about commercial data privacy practices.

V. CONCLUSION

The final privacy framework set forth in this Report reflects the extensive record developed through the Commission's privacy roundtables as well as the over 450 public comments received in response to the proposed framework issued in December of 2010. The FTC recommends that Congress consider baseline privacy legislation while industry implements the final privacy framework through individual company initiatives and through strong and enforceable self-regulatory initiatives. As discussed throughout the report, there are a number of specific areas where policy makers have a role in assisting with the implementation of the self-regulatory principles that make up the privacy framework. Areas where the FTC will be active over the course of the next year include the following.

- **Do Not Track:** As discussed above, industry has made significant progress in implementing Do Not Track. The browser vendors have developed tools that consumers can use to signal that they do not want to be tracked; the DAA has developed its own icon-based tool and has committed to honor the browser tools; and the W3C has made substantial progress in creating an international standard for Do Not Track. However, the work is not done. The Commission will work with these groups to complete implementation of an easy-to use, persistent, and effective Do Not Track system.

362 *Comment of United States Council for International Business*, cmt. #00366, at 4; *Comment of IMS Health*, cmt. #00380, at 5; *Comment of The Privacy Projects*, cmt. #00482, at 2-3.

363 FTC, *Wise Up About Wi-Fi: Tips for Using Public Wireless Networks* (2011), http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt193.shtm; FTC, *Cookies: Leaving a Trail on the Web*, http://onguardonline.gov/articles/0042-cookies-leaving-trail-web; FTC, *Understanding Mobile Apps*, http://onguardonline.gov/articles/0018-understanding-mobile-apps; FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft*, (July 12, 2011), http://www.ftc.gov/bcp/workshops/stolenfutures/.

- **Mobile:** The Commission calls on companies providing mobile services to work toward improved privacy protections, including the development of short, meaningful disclosures. To this end, FTC staff has initiated a project to update its business guidance about online advertising disclosures.[364] As part of this project, staff will host a workshop on May 30, 2012 and will address, among other issues, mobile privacy disclosures and how these disclosures can be short, effective, and accessible to consumers on small screens. The Commission hopes that the workshop will spur further industry self-regulation in this area.
- **Data Brokers:** To address the invisibility of, and consumers' lack of control over, data brokers' collection and use of consumer information, the Commission supports targeted legislation – similar to that contained in several of the data security bills introduced in the 112th Congress – that would provide consumers with access to information about them held by a data broker.[365] To further increase transparency, the Commission calls on data brokers that compile data for marketing purposes to explore creating a centralized website where data brokers could (1) identify themselves to consumers and describe how they collect and use consumer data and (2) detail the access rights and other choices they provide with respect to the consumer data they maintain.
- **Large Platform Providers:** To the extent that large platforms, such as Internet Service Providers, operating systems, browsers, and social media, seek to comprehensively track consumers' online activities, it raises heightened privacy concerns. To further explore privacy and other issues related to this type of comprehensive tracking, FTC staff intends to host a public workshop in the second half of 2012.
- **Promoting enforceable self-regulatory codes:** The Department of Commerce, with the support of key industry stakeholders, is undertaking a project to facilitate the development of sector-specific codes of conduct. FTC staff will participate in that project. To the extent that strong privacy codes are developed, the Commission will view adherence to such codes favorably in connection with its law enforcement work. The Commission will also continue to enforce the FTC Act to take action against companies that engage in unfair or deceptive practices, including the failure to abide by self-regulatory programs they join.

In all other areas, the Commission calls on individual companies, trade associations, and self-regulatory bodies to adopt the principles contained in the privacy framework, to the extent they have not already done so. For its part, the FTC will focus its policy efforts on the five areas identified above, vigorously enforce existing laws, work with industry on self-regulation, and continue to target its education efforts on building awareness of existing data collection and use practices and the tools to control them.

364 *See* Press Release, FTC, FTC Seeks Input to Revising its Guidance to Businesses About Disclosures in Online Advertising (May 26, 2011), *available at* http://www.ftc.gov/opa/2011/05/dotcom.shtm.

365 *See* Data Accountability and Trust Act, H.R. 1707, 112th Congress (2011); Data Accountability and Trust Act of 2011, H.R. 1841, 112th Congress (2011); Data Security and Breach Notification Act of 2011, S. 1207, 112th Congress (2011).

FTC Privacy Milestones

FTC Privacy Milestones

1970	Fair Credit Reporting Act enacted
1972	First Fair Credit Reporting Act (FCRA) case: In the Matter of Credit Bureau of Lorain
1975	FTC sues tax preparer for improperly using customers' information to market its loans: FTC v. Beneficial Corporation
1970s	FTC brings 15 additional enforcement actions against credit bureaus and report users
1983	First FCRA case against a nationwide credit bureau: FTC v. TransUnion
1985	FCRA sweep against users of consumer reports
1990	Commission staff issues comprehensive commentary on the FCRA
1991	FTC sues TRW for FCRA violations: FTC v. TRW
1992	FCRA sweep against employers using credit reports
1995	FTC sues Equifax for FCRA violations: In the Matter of Equifax Credit Information Services
1996	First major revision of the Fair Credit Reporting Act
	FTC sponsors workshop: *Consumer Privacy on the Global Information Infrastructure*
1997	First spam case: FTC v. Nia Cano
	FTC hosts traveling workshops to discuss revisions of FCRA
	FTC sponsors workshop: *Consumer Information Privacy*
	FTC issues *Individual Reference Services: A Federal Trade Commission Report to Congress*
1998	FTC issues *Privacy Online: A Federal Trade Commission Report to Congress*
1999	First case involving children's privacy: In the Matter of Liberty Financial
	First consumer privacy case: In the Matter of GeoCities
	FTC issues *Self-Regulation and Privacy Online: A Federal Trade Commission Report to Congress*
	FTC sponsors workshop: *Online Profiling*
	FTC launches ID Theft website: consumer.gov/idtheft and ID Theft Online Complaint Form
	FTC's 877-ID-THEFT consumer helpline established
2000	Children's Online Privacy Protection Rule (COPPA) goes into effect
	Gramm-Leach-Bliley Financial Privacy Rule goes into effect
	Three nationwide consumer reporting agencies pay $2.5 million in civil penalties for FCRA violations: US v. Equifax Credit Information Services, US v. TransUnion, and US v. Experian Information Solutions
	First COPPA case: FTC v. Toysmart.com
	FTC issues *Online Profiling: A Federal Trade Commission Report to Congress*
	FTC issues *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*

FTC Privacy Milestones
continued

	FTC sponsors workshop: *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*
	FTC publishes ID Theft booklet for victims: *When Bad Things Happen to Your Good Name*
2001	COPPA Safe Harbor Program begins
	First civil penalty cases under COPPA: US v. Looksmart, US v. Monarch Services, US v. Bigmailbox
	FTC sponsors workshops: *The Information Marketplace: Merging and Exchanging Consumer Data*; *Gramm-Leach-Bliley Educational Program on Financial Privacy*; and *Get Noticed: Effective Financial Privacy Notices: An Interagency Workshop*
	FTC publishes ID Theft Affidavit
2002	First data security case: In the Matter of Eli Lilly & Company
	FTC settles data security charges related to Microsoft's Passport service: In the Matter of Microsoft
	FTC sponsors workshop: *Consumer Information Security Workshop*
	FTC issues report on *Public Workshop: The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*
	FTC launches 10-minute educational ID Theft video
	FTC distributes over 1 million ID Theft booklets for victims
2003	Fair and Accurate Credit Transactions Act (FACTA) passed
	National Do Not Call Registry goes into effect
	Gramm-Leach-Bliley Safeguards Rule goes into effect
	FTC sues companies for sharing students' survey data with commercial marketers: In the Matter of Education Research Center of America and Student Marketing Group
	Guess settles FTC data security charges: In the Matter of Guess?
	FTC issues *Technologies for Protecting Personal Information: A Staff Workshop Report*
	FTC sponsors workshops: *Technologies for Protecting Personal Information*; *Spam Forum*; and *Costs and Benefits Related To the Collection and Use of Consumer Information*
2004	CAN-SPAM Rule goes into effect
	CAN-SPAM Adult Labeling Rule goes into effect
	Free Annual Credit Report Rule goes into effect
	First spyware case: FTC v. Seismic Entertainment
	FTC charges company with exposing consumers' purchases: In the Matter of MTS (dba Tower Records)
	FTC charges company with renting consumer information it had pledged to keep private: In the Matter of Gateway Learning

	FTC issues *The CAN-SPAM Act of 2003: National Do Not Email Registry: A Federal Trade Commission Report to Congress*
	FTC sponsors workshops: *Monitoring Software on Your PC: Spyware, Adware and Other Software*; *Radio Frequency IDentification: Applications and Implications for Consumers*; and *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues*
	FTC publishes *The CAN-SPAM Act: A Compliance Guide for Business*
2005	FACTA Disposal Rule goes into effect
	FACTA Pre-Screen Opt Out Rule goes into effect
	National Do Not Call Registry tops 100 million phone numbers
	First Do Not Call enforcement action: FTC v. National Consumer Council
	First Do Not Call civil penalty action: US v. Braglia Marketing
	Highest civil penalty in a Do Not Call case: US v. DirecTV ($5.3 million)
	First enforcement actions under Gramm-Leach-Bliley Safeguards Rule: In the Matter of Sunbelt Lending and In the Matter of Nationwide Mortgage Group
	First unfairness allegation in a data security case: In the Matter of BJ's Wholesale Club
	FTC issues *RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission*
	FTC issues *Spyware Workshop: Monitoring Software On Your Personal Computer: Spyware, Adware, and Other Software: Report of the Federal Trade Commission Staff*
	FTC launches online safety website: OnGuardOnline.gov
2006	FACTA Rule Limiting Marketing Solicitations from Affiliates goes into effect
	Highest civil penalty in a consumer protection case: US v. ChoicePoint ($10 million civil penalty for violations of FCRA as well as $5 million redress for victims)
	First adware case: In the Matter of Zango
	Highest civil penalty to date in a COPPA case: US v. Xanga ($1 million)
	FTC settles charges against a payment processor that had experienced the largest breach of financial data to date: In the Matter of CardSystems Solutions
	FTC issues *Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues: A Federal Trade Commission Staff Workshop Report*
	FTC sponsors workshop: *Protecting Consumers in the Next Tech-Ade*
	FTC launches national educational campaign on identity theft and publishes *Deter, Detect, Defend: Avoid ID Theft* brochure

FTC Privacy Milestones
continued

2007	First Disposal Rule case: US v. American United Mortgage Company
	Adult-oriented online social networking operation settles FTC charges; unwitting consumers pelted with sexually graphic pop-ups: FTC v. Various (dba AdultFriendFinder)
	FTC issues *Spam Summit: The Next Generation of Threats and Solutions: A Staff Report by the Federal Trade Commission's Division of Marketing Practices*
	FTC issues *Implementing the Children's Online Privacy Protection Act: A Federal Trade Commission Report to Congress*
	FTC co-chairs President's Identity Theft Task Force (with DOJ) and issues Strategic Plan
	FTC sponsors workshops: *Security in Numbers: SSNs and ID Theft; Ehavioral Advertising: Tracking, Targeting, and Technology*; and *Spam Summit: The Next Generation of Threats and Solutions*
	FTC publishes *Protecting Personal Information: A Guide for Business* and launches interactive tutorial
2008	Highest civil penalty in a CAN-SPAM case: US v. ValueClick ($2.9 million)
	FTC settles charges against data broker Lexis Nexis and retailer TJX related to the compromise of hundreds of thousands of consumers' information: In the Matter of Reed Elsevier and Seisent and In the Matter of TJX Companies
	FTC issues *Protecting Consumers in the Next Tech-ade: A Report by the Staff of the Federal Trade Commission*
	FTC issues *Security In Numbers: Social Security Numbers and Identity Theft – A Federal Trade Commission Report Providing Recommendations On Social Security Number Use In the Private Sector*
	President's Identity Theft Task Force Report released
	FTC sponsors workshops: *Protecting Personal Information: Best Practices for Business* (Chicago, Dallas, and Los Angeles); *Pay on the Go: Consumers and Contactless Payment, Transatlantic RFID Workshop on Consumer Privacy and Data Security*; and *Beyond Voice: Mapping the Mobile Marketplace*
	U.S. Postal Service sends FTC ID Theft prevention brochure to every household in the country
2009	Robocall Rule goes into effect
	Health Breach Notification Rule goes into effect
	First case alleging failure to protect employee information: In the Matter of CVS Caremark
	First cases alleging six companies violated the EU-US Safe Harbor Agreement: In the Matter of World Innovators, In the Matter of ExpatEdge Partners, In the Matter of Onyx Graphics, In the Matter of Directors Desk, In the Matter of Progressive Gaitways, and In the Matter of Collectify
	FTC issues *Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology*

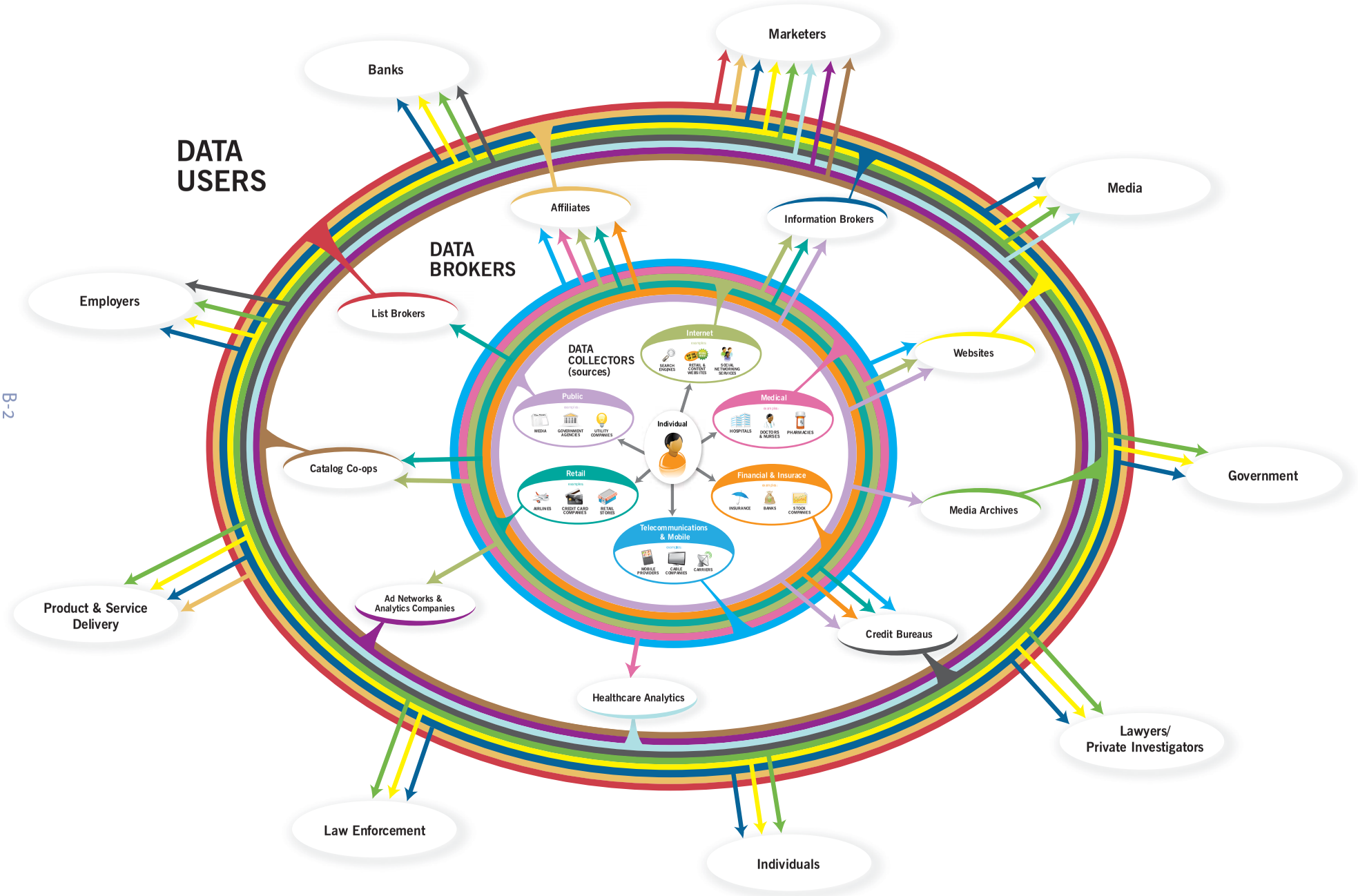
	FTC sponsors workshops: *Exploring Privacy: A Roundtable Series*; *Protecting Personal Information: Best Practices for Business* (New York); and *Securing Personal Data in the Global Economy*
	FTC publishes *Net Cetera: Chatting with Kids About Being Online*
2010	FTC jointly publishes Model Privacy Form under the Gramm-Leach-Bliley Act
	National Do Not Call Registry tops 200 million phone numbers
	First data security case involving social media: In the Matter of Twitter
	First case shutting down a rogue ISP: FTC v. Pricewert
	First data security case against an online seal provider: FTC v. ControlScan
	Highest judgment in a spyware case: FTC v. Innovative Marketing ($163 million)
	Largest FTC-state coordinated settlement on privacy: FTC v. Lifelock
	FTC conducts sweep against companies for exposure of employee and/or customer data on peer-to-peer (P2P) file-sharing networks
	FTC releases Preliminary FTC Staff Report *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*
	FTC sponsors *COPPA Rule Review Roundtable*
	FTC publishes *Peer-to-Peer File Sharing: A Guide for Businesses*; *Medical Identity Theft: How to Minimize Your Risk*; and *Copier Data Security: A Guide for Businesses*
	FTC distributes 6+ million printed copies of *Deter, Detect, Defend: Avoid ID Theft* brochures and 5+ million printed copies of *Net Cetera: Chatting with Kids About Being Online*
2011	FTC seeks comment on proposed changes to COPPA rule
	First case alleging substantive Safe Harbor violation and imposing privacy assessment program and audit requirements: In the Matter of Google
	First case against an online advertising network for offering deceptive privacy controls: In the Matter of Chitika
	First COPPA case against a mobile application developer: US v. W3 Innovations
	First case alleging unfairness based on default privacy settings: FTC v. Frostwire
	Largest FTC privacy case to date: In the Matter of Facebook
	FTC releases report *40 Years of Experience with the Fair Credit Reporting Act*
	FTC co-hosts *Stolen Futures: A Forum on Child ID Theft*
	FTC hosts *Face Facts: A Forum on Facial Recognition* Workshop
	FTC publishes *Tips for Using Public Wireless Networks*
	FTC publishes *Facts from the FTC: What You Should Know About Mobile Apps*
	FTC publishes *Online Safety for Teens and Tweens*

FTC Privacy Milestones
continued

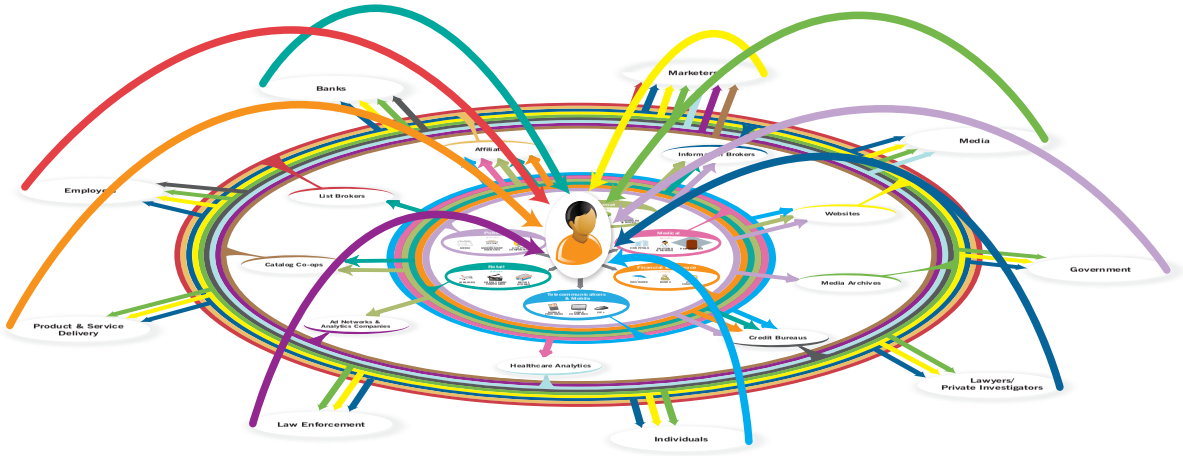
2012	Reports	FTC releases report *Using FACTA Remedies: An FTC Staff Report on a Survey of Identity Theft Victims*
	Reports	FTC releases report *Mobile Apps for Kids: Current Privacy Disclosures Are Disappointing*
	Workshops	FTC announces workshop: *Paper, Plastic... or Mobile? An FTC Workshop on Mobile Payments*
	Workshops	FTC announces workshop to Explore Disclosures in Online and Mobile Media
	Education	FTC publishes Blog Post: *FCRA & Mobile Apps: A Word of Warning*

Personal Data Ecosystem

Personal Data Ecosystem



DATA USES:



Examples of uses of consumer information in personally identifiable or aggregated form:

- Financial services, such as for banking or investment accounts
- Credit granting, such as for credit or debit cards; mortgage, automobile or specialty loans; automobile rentals; or telephone services
- Insurance granting, such as for health, automobile or life
- Retail coupons and special offers
- Catalog and magazine solicitations
- Web and mobile services, including content, e-mail, search, and social networking
- Product and service delivery, such as streaming video, package delivery, or a cable signal
- Attorneys, such as for case investigations
- Journalism, such as for fact checking
- Marketing, whether electronically, through direct mail, or by telephone
- Data brokers for aggregation and resale to companies and/or consumers
- Background investigations by employers or landlords
- Locating missing or lost persons, beneficiaries, or witnesses
- Law enforcement
- Research (e.g., health, financial, and online search data) by academic institutions, government agencies, and commercial companies
- Fraud detection and prevention
- Government benefits and services, such as licensing

Dissenting Statement of Commissioner J. Thomas Rosch

Dissenting Statement of Commissioner J. Thomas Rosch
Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers
March 26, 2012

Introduction

I agree in several respects with what the "final" Privacy Report says. Specifically, although I disagree that the consumer has traditionally ever been given any "choice" about information collection practices (other than to "take-it-or-leave-it" after reviewing a firm's privacy notice), I agree that consumers ought to be given a broader range of choices if for no other reason than to customize their privacy protection. However, I still worry about the constitutionality of banning take-it-or-leave-it choice (in circumstances where the consumer has few alternatives); as a practical matter, that prohibition may chill information collection, and thus impact innovation, regardless whether one's privacy policy is deceptive or not.[1]

I also applaud the Report's recommendation that Congress enact "targeted" legislation giving consumers "access" to correct misinformation about them held by a data broker.[2] I also support the Report's recommendation that Congress implement federal legislation that would require entities to maintain reasonable security and to notify consumers in the event of certain security breaches.[3]

Finally, I concur with the Report insofar as it recommends that information brokers who compile data for marketing purposes must disclose to consumers how they collect and use consumer data.[4] I have long felt that we had no business counseling Congress or other agencies about privacy concerns without that information. Although I have suggested that compulsory process be used to obtain such information (because I am convinced that is the only way to ensure that our information is complete and accurate),[5] a voluntary centralized website is arguably a step in the right direction.

Privacy Framework

My disagreement with the "final" Privacy Report is fourfold. First, the Report is rooted in its insistence that the "unfair" prong, rather than the "deceptive" prong, of the Commission's Section 5 consumer protection statute, should govern information gathering practices (including "tracking"). "Unfairness" is an elastic and elusive concept. What is "unfair" is in the eye of the beholder. For example, most consumer advocacy groups consider behavioral tracking to be unfair, whether or not the information being tracked is personally identifiable ("PII") and regardless of the circumstances under which an entity does the

1 *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* ("Report") at 50-52.

2 *Id.* at 14, 73.

3 *Id.* at 26. I also support the recommendation that such legislation authorize the Commission to seek civil penalties for violations. However, despite its bow to "targeted" legislation, the Report elsewhere counsels that the Commission support privacy legislation generally. *See, e.g.*, *id.* at 16. To the extent that those recommendations are not defined, or narrowly targeted, I disagree with them.

4 *Id.* at 14, 68-70.

5 *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Information and Privacy: In Search of a Data-Driven Policy, Remarks at the Technology Policy Institute Aspen Forum (Aug. 22, 2011), *available at* http://www.ftc.gov/speeches/rosch/110822aspeninfospeech.pdf.

tracking. But, as I have said, consumer surveys are inconclusive, and individual consumers by and large do not "opt out" from tracking when given the chance to do so.[6] Not surprisingly, large enterprises in highly concentrated industries, which may be tempted to raise the privacy bar so high that it will disadvantage rivals, also support adopting more stringent privacy principles.[7]

The "final" Privacy Report (incorporating the preliminary staff report) repeatedly sides with consumer organizations and large enterprises. It proceeds on the premise that behavioral tracking is "unfair."[8] Thus, the Report expressly recommends that "reputational harm" be considered a type of harm that the Commission should redress.[9] The Report also expressly says that privacy be the default setting for commercial data practices.[10] Indeed, the Report says that the "traditional distinction between PII and non-PII has blurred,"[11] and it recommends "shifting the burdens away from consumers and placing obligations on businesses."[12] To the extent the Report seeks consistency with international privacy standards,[13] I would urge caution. We should always carefully consider whether each individual policy choice regarding privacy is appropriate for this country in all contexts.

That is not how the Commission itself has traditionally proceeded. To the contrary, the Commission represented in its 1980, and 1982, Statements to Congress that, absent deception, it will not generally enforce Section 5 against alleged intangible harm.[14] In other contexts, the Commission has tried, through its advocacy, to convince others that our policy judgments are sensible and ought to be adopted. And, as I stated in connection with the recent *Intel* complaint, in the competition context, one of the principal virtues

6 *See* Katy Bachman, *Study: Internet User Adoption of DNT Hard to Predict*, adweek.com, March 20, 2012, *available at* http://www.adweek.com/news/technology/study-internet-user-adoption-dnt-hard-predict-139091 (reporting on a survey that found that what Internet users say they are going to do about using a Do Not Track button and what they are currently doing about blocking tracking on the Internet, are two different things); s*ee also* Concurring Statement of Commissioner J. Thomas Rosch, Issuance of Preliminary FTC Staff Report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (Dec. 1, 2010), *available at* http://www.ftc.gov/speeches/rosch/101201privacyreport.pdf.

7 *See* J. Thomas Rosch, Comm'r, Fed. Trade Comm'n, Do Not Track: Privacy in an Internet Age, Remarks at Loyola Chicago Antitrust Institute Forum, (Oct. 14, 2011), *available at* http://www.ftc.gov/speeches/rosch/111014-dnt-loyola.pdf; *see also* Report at 9.

8 Report at 8 and n.37.

9 *Id*. at 2. The Report seems to imply that the Do Not Call Rule would support this extension of the definition of harm. *See id*. ("unwarranted intrusions into their daily lives"). However, it must be emphasized that the *Congress* granted the FTC underlying authority under the Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108, to promulgate the Do Not Call provisions and other substantial amendments to the TSR. The Commission did not do so unilaterally.

10 *Id*.

11 *Id*. at 19.

12 *Id*. at 23, *see also id.* at 24.

13 *Id*. at 9-10. This does not mean that I am an isolationist or am impervious to the benefits of a global solution. But, as stated below, there is more than one way to skin this cat.

14 *See* Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Committee on Commerce, Science and Transportation, United States Senate, Commission Statement of Policy on the Scope of Consumer Unfairness Jurisdiction (Dec. 17, 1980), reprinted in International Harvester Co., 104 F.T.C. 949, 1070, 1073 (1984) ("Unfairness Policy Statement") *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm; Letter from the FTC to Hon. Bob Packwood and Hon. Bob Kasten, Committee on Commerce, Science and Transportation, United States Senate, reprinted in FTC Antitrust & Trade Reg. Rep. (BNA) 1055, at 568-570 ("Packwood-Kasten letter"); and 15 U.S.C. § 45(n), which codified the FTC's modern approach.

of applying Section 5 was that that provision was "self-limiting," and I advocated that Section 5 be applied on a stand-alone basis only to a firm with monopoly or near-monopoly power.[15] Indeed, as I have remarked, absent such a limiting principle, privacy may be used as a weapon by firms having monopoly or near-monopoly power.[16]

There does not appear to be any such limiting principle applicable to many of the recommendations of the Report. If implemented as written, many of the Report's recommendations would instead apply to almost all firms and to most information collection practices. It would install "Big Brother" as the watchdog over these practices not only in the online world but in the offline world.[17] That is not only paternalistic, but it goes well beyond what the Commission said in the early 1980s that it would do, and well beyond what Congress has permitted the Commission to do under Section 5(n).[18] I would instead stand by what we have said and challenge information collection practices, including behavioral tracking, only when these practices are deceptive, "unfair" within the strictures of Section 5(n) and our commitments to Congress, or employed by a firm with market power and therefore challengeable on a stand-alone basis under Section 5's prohibition of unfair methods of competition.

Second, the current self-regulation and browser mechanisms for implementing Do Not Track solutions may have advanced since the issuance of the preliminary staff Report.[19] But, as the final Report concedes, they are far from perfect,[20] and they may never be, despite efforts to create a standard through the World Wide Web Consortium ("W3C") for the browser mechanism.[21]

More specifically, as I have said before, the major browser firms' interest in developing Do Not Track mechanisms begs the question of whether and to what extent those major browser firms will act strategically and opportunistically (to use privacy to protect their own entrenched interests).[22]

In addition, the recent announcement by the Digital Advertising Alliance (DAA) that it will honor the tracking choices consumers make through their browsers raises more questions than answers for me. The Report is not clear, and I am concerned, about the extent to which this latest initiative will displace the standard-setting effort that has recently been undertaken by the W3C. Furthermore, it is not clear that all the interested players in the Do Not Track arena – whether it be the DAA, the browser firms, the W3C, or consumer advocacy groups – will be able to come to agreement about what "Do Not Track" even means.[23] It may be that the firms professing an interest in self-regulation are really talking about a "Do Not Target" mechanism, which would only prevent a firm from serving targeted ads, rather than a "Do Not Track"

15 *See* Concurring and Dissenting Statement of Commissioner J. Thomas Rosch, *In re Intel Corp*., Docket No. 9341, (Dec. 16, 2009), *available at* http://www.ftc.gov/os/adjpro/d9341/091216intelstatement.pdf.

16 *See* Rosch, *supra* note 7 at 20.

17 *See* Report at 13.

18 Federal Trade Commission Act Amendments of 1994, Pub. L. No. 103-312.

19 Report at 4, 52.

20 *Id*. at 53, 54; *see esp. id*. at 53 n.250.

21 *Id*. at 5, 54.

22 *See* Rosch, *supra* note 7 at 20-21.

23 Tony Romm, "*What Exactly Does 'Do Not Track' Mean?*," Politico, Mar. 13, 2012, *available at* http://www.politico.com/news/stories/0312/73976.html; *see also* Report at 4 (DAA allows consumer to opt out of "targeted advertising").

mechanism, which would prevent the collection of consumer data altogether. For example, the DAA's Self-Regulatory Principles for Multi-Site Data do not apply to data collected for "market research" or "product development."[24] For their part, the major consumer advocacy groups may not be interested in a true "Do Not Track" mechanism either. They may only be interested in a mechanism that prevents data brokers from compiling consumer profiles instead of a comprehensive solution. It is hard to see how the W3C can adopt a standard unless and until there is an agreement about what the standard is supposed to prevent.[25]

It is also not clear whether or to what extent the lessons of the Carnegie Mellon Study respecting the lack of consumer understanding of how to access and use Do Not Track will be heeded.[26] Similarly, it is not clear whether and to what extent Commissioner Brill's concern that consumers' choices, whether it be "Do Not Collect" or merely "Do Not Target," will be honored.[27] Along the same lines, it is also not clear whether and to what extent a "partial" Do Not Track solution (offering nuanced choice) will be offered or whether it is "all or nothing." Indeed, it is not clear whether consumers can or will be given complete and accurate information about the pros and the cons of subscribing to Do Not Track before they choose it. I find this last question especially vexing in light of a recent study that indicated 84% of users polled prefer targeted advertising in exchange for free online content.[28]

Third, I am concerned that "opt-in" will necessarily be selected as the *de facto* method of consumer choice for a wide swath of entities that have a first-party relationship with consumers but who can potentially track consumers' activities across unrelated websites, under circumstances where it is unlikely, because of the "context" (which is undefined) for such tracking to be "consistent" (which is undefined) with that first-party relationship:[29] 1) companies with multiple lines of business that allow data collection in different contexts (such as Google);[30] 2) "social networks," (such as Facebook and Twitter), which could potentially use "cookies," "plug-ins," applications, or other mechanisms to track a consumer's activities across

24 *See Self-Regulatory Principles for Multi-Site Data,* Digital Advertising Alliance, Nov. 2011, at 3, 10, 11, *available at* http://www.aboutads.info/resource/download/Multi-Site-Data-Principles.pdf; *see also* Tanzina Vega, *Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, New York Times, Feb. 26, 2012, *available at* http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-web-tracking.html?pagewanted=all.

25 *See* Vega, *supra* note 24.

26 *"Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*," Carnegie Mellon University CyLab, Oct. 31, 2011, *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab11017.pdf; *see also Search Engine Use 2012,* at 25, Pew Internet & American Life Project, Pew Research Center, Mar. 9, 2012, *available at* http://pewinternet.org/~/media/Files/Reports/2012/PIP_Search_Engine_Use_2012.pdf ("[j]ust 38% of internet users say they are generally aware of ways they themselves can limit how much information about them is collected by a website").

27 *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Big Data, Big Issues, Remarks at Fordham University School of Law (Mar. 2, 2012) *available at* http://www.ftc.gov/speeches/brill/120228fordhamlawschool.pdf.

28 *See* Bachman, *supra* note 6.

29 Report at 41.

30 *Id.* Notwithstanding that Google's prospective conduct seems to fit perfectly the circumstances set forth on this page of the Report (describing a company with multiple lines of business including a search engine and ad network), where the Commission states "consumer choice" is warranted, the Report goes on to conclude on page 56 that Google's practices do not require affirmative express consent because they "currently are not so widespread that they could track a consumer's every movement across the Internet."

the Internet;[31] and 3) "retargeters," (such as Amazon or Pacers), which include a retailer who delivers an ad on a third-party website based on the consumer's previous activity on the retailer's website.[32]

These entities might have to give consumers "opt-in" choice now or in the future: 1) regardless whether the entity's privacy policy and notices adequately describe the information collection practices at issue; 2) regardless of the sensitivity of the information being collected; 3) regardless whether the consumer cares whether "tracking" is actually occurring; 4) regardless of the entity's market position (whether the entity can use privacy strategically – *i.e.*, an opt-in requirement – in order to cripple or eliminate a rival); and 5) conversely, regardless whether the entity can compete effectively or innovate, as a practical matter, if it must offer "opt in" choice.[33]

Fourth, I question the Report's apparent mandate that ISPs, with respect to uses of deep packet inspection, be required to use opt-in choice.[34] This is not to say there is no basis for requiring ISPs to use opt-in choice without requiring opt-in choice for other large platform providers. But that kind of "discrimination" cannot be justified, as the Report says, because ISPs have "are in a position to develop highly detailed and comprehensive profiles of their customers."[35] So does any large platform provider who makes available a browser or operating system to consumers.[36]

Nor can that "discrimination" be justified on the ground that ISPs may potentially use that data to "track" customer behavior in a fashion that is contrary to consumer expectations. There is no reliable data establishing that most ISPs presently do so. Indeed, with a business model based on subscription revenue, ISPs arguably lack the same incentives as do other platform providers whose business model is based on attracting advertising and advertising revenue: ISPs assert that they track data only to perform operational and security functions; whereas other platform providers that have business models based on advertising revenue track data in order to maximize their advertising revenue.

What really distinguishes ISPs from most other "large platform providers" is that their markets can be highly concentrated.[37] Moreover, even when an ISP operates in a less concentrated market, switching costs can be, or can be perceived as being, high.[38] As I said in connection with the *Intel* complaint, a monopolist or near monopolist may have obligations which others do not have.[39] The only similarly situated platform provider may be Google, which, because of its alleged monopoly power in the search advertising market,

31 *Id.* at 40. *See also supra* note 30. That observation also applies to "social networks" like Facebook.

32 *Id*. at 41.

33 *See id.* at 60 ("Final Principle").

34 *Id*. at 56 ("the Commission has strong concerns about the use of DPI for purposes inconsistent with an ISP's interaction with a consumer, without express affirmative consent or more robust protection").

35 *Id*.

36 *Id.*

37 Federal Communications Commission, *Connecting America: The National Broadband Plan, Broadband Competition and Innovation Policy, Section 4.1, Networks, Competition in Residential Broadband Markets* at 36, *available at* http://www.broadband.gov/plan/4-broadband-competition-and-innovation-policy/.

38 Federal Communications Commission Working Paper, *Broadband decisions: What drives consumers to switch – or stick with – their broadband Internet provider* (Dec. 2010), at 3, 8, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2010/db1206/DOC-303264A1.pdf.

39 *See* Rosch, *supra* note 15.

has similar power. For any of these "large platform providers," however, affirmative express consent should be required only when the provider *actually* wants to use the data in this fashion, not just when it *has the potential* to do so.[40]

Conclusion

Although the Chairman testified recently before the House Appropriations Subcommittee chaired by Congresswoman Emerson that the recommendations of the final Report are supposed to be nothing more than "best practices,"[41] I am concerned that the language of the Report indicates otherwise, and broadly hints at the prospect of enforcement.[42] The Report also acknowledges that it is intended to serve as a template for legislative recommendations.[43] Moreover, to the extent that the Report's "best practices" mirror the Administration's privacy "Bill of Rights," the President has specifically asked either that the "Bill of Rights" be adopted by the Congress or that they be distilled into "enforceable codes of conduct."[44] As I testified before the same subcommittee, this is a "tautology;" either these practices are to be adopted voluntarily by the firms involved or else there is a federal requirement that they be adopted, in which case there can be no pretense that they are "voluntary."[45] It makes no difference whether the federal requirement is in the form of enforceable codes of conduct or in the form of an act of Congress. Indeed, it is arguable that neither is needed if these firms feel obliged to comply with the "best practices" or face the wrath of "the Commission" or its staff.

40 *See, e.g.*, Report at 56.

41 Testimony of Jon Leibowitz and J. Thomas Rosch, Chairman and Comm'r, FTC, *The FTC in FY2013: Protecting Consumers and Competition*: *Hearing on Budget Before the H. Comm. on Appropriations Subcomm. on Financial Services and General Government*, 112 th Cong. 2 (2012), text from CQ Roll Call, available from: LexisNexis® Congressional.

42 One notable example is found where the Report discusses the articulation of privacy harms and enforcement actions brought on the basis of *deception*. The Report then notes "[l]ike these enforcement actions, a privacy framework should address practices that unexpectedly reveal previously private information even absent physical or financial harm, or unwarranted intrusions." Report at 8. The accompanying footnote concludes that "even in the absence of such misrepresentations, revealing previously-private consumer data could cause consumer harm." *See also infra* note 43.

43 *Id*. at 16 ("to the extent Congress enacts any of the Commission's recommendations through legislation"); *see also id*. at 12-13 ("the Commission calls on Congress to develop baseline privacy legislation that is technologically neutral and sufficiently flexible to allow companies to continue to innovate").

44 *See* Letter from President Barack Obama, *appended to* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

45 *See* FTC Testimony, *supra* note 41.

122 3090

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET NO. C-4426**
TRENDNET, INC.,	)	
a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that TRENDnet, Inc., a corporation, has violated the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent TRENDnet, Inc. ("TRENDnet" or "respondent") is a California corporation with its principal office or place of business at 20675 Manhattan Place, Torrance, California 90501.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Respondent is a retailer that among other things, sells networking devices, such as routers, modems, and Internet Protocol ("IP") cameras, to home users and to small- and medium-sized businesses. In 2010, respondent had approximately $64 million in total revenue, and obtained approximately $6.3 million of this amount from the sale of IP cameras. In 2011, respondent had approximately $66 million in total revenue and obtained approximately $5.28 million of this amount from the sale of its IP cameras. Similarly, in 2012, the company had approximately $62 million in total revenue and obtained approximately $7.4 million of this amount from the sale of IP cameras. During this time, the company had approximately 80 employees.

4. Respondent offers its IP cameras for consumers to conduct security monitoring of their homes or businesses, by accessing live video and audio feeds ("live feeds") from their cameras over the Internet. In many instances, these cameras are marketed under the trade name "SecurView." According to respondent, the IP cameras may be used to monitor "babies at home, patients in the hospital, offices and banks, and more."

5. By default, respondent has required users to enter a user name and password ("login credentials"), in order to access the live feeds from their cameras over the Internet. In addition, since at least February 2010, respondent has provided users with a Direct Video Stream Authentication setting ("DVSA setting"), the same as or similar to the one depicted below. The DVSA setting allows users to turn off the login credentials requirement for their cameras, so that they can make their live feeds public. To remove the login credentials requirement, a user would uncheck the box next to the word "Enable," and then "Apply" this selection.

6. Respondent also has provided software applications that enable users to access their live feeds from a mobile device ("mobile apps"), including its SecurView Mobile Android app, which respondent launched in January 2011, and its SecurView PRO Android app, which respondent launched in October 2012. Both apps require that a user enter login credentials the first time that the user employs the app on a particular mobile device. Both apps then store the user's login credentials on that mobile device, so that the user will not be required to enter login credentials on that device in the future.

RESPONDENT'S STATEMENTS TO CONSUMERS

7. From at least January 1, 2010, until the present, in many instances, in marketing or offering for sale its IP cameras, respondent has:

    a. used the trade name SecurView:

        i. in the product names and descriptions displayed on the cameras' packaging (*see, e.g.*, Exhs. A-J);

        ii. in product descriptions on respondent's website and in other advertisements (*see, e.g.*, Exhs. K-L); and

        iii. in the name of its SecurView Mobile and SecurView PRO Android apps, described in **Paragraph 6**.

    b. described the IP cameras as "secure" or suitable for maintaining security, including through:

        i. a sticker affixed to the cameras' packaging, the same as or similar to the one depicted below, which displays a lock icon and the word "security" (*see, e.g.*, Exhs. B, D, F-H, J);

        ii. a statement on the cameras' packaging that it may be used to "secure," or "protect" a user's home, family, property, or business (*see, e.g.*, Exhs. A, B, I); and

        iii. product descriptions on respondent's website and in other advertisements (*see, e.g.*, Exhs. K-M);

    c. provided an authentication feature, which requires users to enter login credentials before accessing the live feeds from their IP cameras over the Internet; and

d. provided the DVSA setting, described in **Paragraph 5**, which purports to allow users to choose whether login credentials will be required to access the live feeds from their IP cameras over the Internet.

RESPONDENT'S FAILURE TO REASONABLY SECURE ITS IP CAMERAS AGAINST UNAUTHORIZED ACCESS

8. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security to prevent unauthorized access to sensitive information, namely the live feeds from the IP cameras. Among other things:

    a. since at least April 2010, respondent has transmitted user login credentials in clear, readable text over the Internet, despite the existence of free software, publicly available since at least 2008, that would have enabled respondent to secure such transmissions;

    b. since January 2011, respondent has stored user login credentials in clear, readable text on a user's mobile device, despite the existence of free software, publicly available since at least 2008, that would have enabled respondent to secure such stored credentials;

    c. since at least April 2010, respondent has failed to implement a process to actively monitor security vulnerability reports from third-party researchers, academics, or other members of the public, despite the existence of free tools to conduct such monitoring, thereby delaying the opportunity to correct discovered vulnerabilities or respond to incidents;

    d. since at least April 2010, respondent has failed to employ reasonable and appropriate security in the design and testing of the software that it provided consumers for its IP cameras. Among other things, respondent, either directly or through its service providers, failed to:

        i. perform security review and testing of the software at key points, such as upon the release of the IP camera or upon the release of software for the IP camera, through measures such as:

            1. a security architecture review to evaluate the effectiveness of the software's security;

            2. vulnerability and penetration testing of the software, such as by inputting invalid, unanticipated, or random data to the software;

            3. reasonable and appropriate code review and testing of the software to verify that access to data is restricted consistent with a user's privacy and security settings; and

ii. implement reasonable guidance or training for any employees responsible for testing, designing, and reviewing the security of its IP cameras and related software.

RESPONDENT'S BREACH

9. As a result of the failures described in **Paragraph 8**, respondent has subjected its users to a significant risk that their sensitive information, namely the live feeds from its IP cameras, will be subject to unauthorized access. As a result of the failures described in **Paragraph 8(d)**, from approximately April 2010 until February 7, 2012, the DVSA setting, described in **Paragraph 5**, did not function properly for twenty models of respondent's IP cameras. (*See* Appendix A, listing the affected models.) In particular, the DVSA setting failed to honor a user's choice to require login credentials and allowed all users' live feeds to be publicly accessible, regardless of the choice reflected by a user's DVSA setting and with no notice to the user.

10. Hackers could and did exploit the vulnerability described in **Paragraph 9**, to compromise hundreds of respondent's IP cameras. Specifically, on approximately January 10, 2012, a hacker visited respondent's website and reviewed the software that respondent makes available for its cameras. The hacker was able to identify a web address that appeared to support the public sharing of users' live feeds, for those users who had made their feeds public. Because of the flaw in respondent's DVSA setting, however, the hacker could access all live feeds at this web address, without entering login credentials, even for users who had not made their feeds public. Thereafter, by typing the term "netcam" into a popular search engine that enables users to search for computers based on certain criteria, such as location or software, the hacker identified and obtained IP addresses for hundreds of respondent's IP cameras that could be compromised. The hacker posted information about the breach online; thereafter, hackers posted links to the live feeds for nearly 700 of respondent's IP cameras. Among other things, these compromised live feeds displayed private areas of users' homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities. The breach was widely reported in news articles online, many of which featured photos taken from the compromised live feeds or hyperlinks to access such feeds. Based on the cameras' IP addresses, news stories also depicted the geographical location (*e.g.*, city and state) of many of the compromised cameras.

11. Respondent learned of the breach on January 13, 2012, when a customer who had read about the breach contacted respondent's technical support staff to report the issue. Shortly thereafter, respondent made available new software to eliminate the vulnerability, and encouraged users to install the new software by posting notices on its website and sending emails to registered users.

THE IMPACT OF RESPONDENT'S FAILURES ON CONSUMERS

12. As demonstrated by the breach, respondent's failures to provide reasonable and appropriate security led to a significant risk that users' live feeds would be compromised, thereby causing significant injury to consumers.

13. The exposure of sensitive information through respondent's IP cameras increases the likelihood that consumers or their property will be targeted for theft or other criminal activity, increases the likelihood that consumers' personal activities and conversations or those of their family members, including young children, will be observed and recorded by strangers over the Internet. This risk impairs consumers' peaceful enjoyment of their homes, increases consumers' susceptibility to physical tracking or stalking, and reduces consumers' ability to control the dissemination of personal or proprietary information (*e.g.*, intimate video and audio feeds or images and conversations from business properties). Consumers had little, if any, reason to know that their information was at risk, particularly those consumers who maintained login credentials for their cameras or who were merely unwitting third parties present in locations under surveillance by the cameras.

COUNT 1

14. As described in **Paragraph 7**, respondent has represented, expressly or by implication, that respondent has taken reasonable steps to ensure that its IP cameras and mobile apps are a secure means to monitor private areas of a consumer's home or workplace.

15. In truth and in fact, as described in **Paragraphs 8-11**, respondent has not taken reasonable steps to ensure that its IP cameras are a secure means to monitor private areas of a consumer's home or workplace. Therefore, the representation set forth in **Paragraph 14** constitutes a false or misleading representation.

COUNT 2

16. As described in **Paragraphs 5 and 7**, respondent has represented, expressly or by implication, that respondent has taken reasonable steps to ensure that a user's security settings will be honored.

17. In truth and in fact, as described in **Paragraphs 8-11**, respondent has not taken reasonable steps to ensure that a user's security settings will be honored. Therefore, the representation set forth in **Paragraph 16** constitutes a false or misleading representation.

COUNT 3

18. As set forth in **Paragraphs 8-11**, respondent has failed to provide reasonable security to prevent unauthorized access to the live feeds from its IP cameras, which respondent offered to consumers for the purpose of monitoring and securing private areas of their homes and businesses. Respondent's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers. This practice was, and is, an unfair act or practice.

19. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this sixteenth day of January, 2014, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL:

COMPLAINT APPENDIX A

1. TV-IP110 (Version A1.xR)
2. TV-IP110W (Version A1.xR)
3. TV-IP110WN (Versions A1.xR & V2.0R)
4. TV-IP121W (Version A1.xR)
5. TV-IP121WN (Versions V1.0R & V2.0R)
6. TV-IP212 (Version A1.xR)
7. TV-IP212W (Version A1.xR)
8. TV-IP252P (Version B1.xR)
9. TV-IP312 (Version A1.xR)
10. TV-IP312W (Version A1.xr)
11. TV-IP312WN (Version A1.xR)
12. TV-IP322P (Version V1.0R)
13. TV-IP410 (Version A1.XR)
14. TV-IP410W (Version A1.xR)
15. TV-IP410WN (Version V1.0R)
16. TV-IP422 (Versions A1.xR & A2.xR)
17. TV-IP422W (Versions A1.xR & A2.xR)
18. TV-IP422WN (Version V1.0R)
19. TV-VS1 (Version V1.0R)
20. TV-VS1P (Version V1.0R)

122 3090

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of	)	**DOCKET No. C-4426**
TRENDNET, INC., a corporation.	)	**DECISION AND ORDER**

The Federal Trade Commission ("Commission" or "FTC"), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 *et seq.*;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Decision and Order ("Order"):

1. Respondent TRENDnet, Inc. ("TRENDnet") is a California corporation with its principal office or place of business at 20675 Manhattan Place, Torrance, California 90501.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. "Affected Consumers" shall mean persons who purchased and installed one of the following Cameras with software last updated prior to February 7, 2012: TV-IP110 (Version A1.xR); TV-IP110W (Version A1.xR); TV-IP110WN (Version A1.xR); TV-IP110WN (Version V2.0R); TV-IP121W (Version A1.xR); TV-IP121WN (Version V1.0R); TV-IP121WN (Version V2.0R); TV-IP212 (Version A1.xR); TV-IP212W (Version A1.xR); TV-IP252P (Version B1.xR); TV-IP312 (Version A1.xR); TV-IP312W (Version A1.xr); TV-IP312WN (Version A1.xR); TV-IP322P (Version V1.0R); TV-IP410 (Version A1.XR); TV-IP410W (Version A1.xR); TV-IP410WN (Version V1.0R); TV-IP422 (Versions A1.xR/A2.xR); TV-IP422W (Versions A1.xR/A2.xR); TV-IP422WN (Version V1.0R); TV-VS1 (Version V1.0R); and TV-VS1P (Version V1.0R).

2. "App" or "Apps" shall mean any software application or related code developed, branded, or provided by respondent for a mobile device, including, but not limited to, any iPhone, iPod touch, iPad, BlackBerry, Android, Amazon Kindle, or Microsoft Windows device.

3. "Cameras" shall mean any Internet Protocol ("IP") camera, cloud camera, or other Internet-accessible camera advertised, developed, branded, or sold by respondent, or on behalf of respondent, or any corporation, subsidiary, division or affiliate owned or controlled by respondent that transmits, or allows for the transmission of Live Feed Information over the Internet.

4. "Clear(ly) and prominent(ly)" shall mean:

   A. In textual communications (*e.g.*, printed publications or words displayed on the screen of a computer or device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;

   B. In communications disseminated orally or through audible means (*e.g.*, radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;

C. In communications disseminated through video means (*e.g.*, television or streaming video), the required disclosures are in writing in a form consistent with subparagraph (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and

D. In all instances, the required disclosures (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any other statements or disclosures provided by respondent.

5. "Commerce" shall mean commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation, as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

6. "Covered Device" shall mean: (1) any Internet-accessible electronic product or device, including but not limited to "Cameras," advertised, developed, branded, or sold by respondent, or on behalf of respondent, or any corporation, subsidiary, division or affiliate owned or controlled by respondent that transmits or allows for the transmission of Covered Information over the Internet; and (2) any App or software advertised, developed, branded, or provided by respondent or any corporation, subsidiary, division or affiliate owned or controlled by respondent used to operate, manage, access, or view the product or device.

7. "Covered Device Functionality" shall mean any capability of a Covered Device to capture, access, store, or transmit Covered Information.

8. "Covered Information" shall mean individually-identifiable information from or about an individual consumer input into, stored on, captured with, accessed, or transmitted through a Covered Device, including but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as a user identifier or screen name; (d) photos; (e) videos; (f) pre-recorded and live-streaming audio; (g) an IP address, User ID or other persistent identifier; or (h) an authentication credential, such as a username or password.

9. "Live Feed Information" shall mean video, audio, or audiovisual data.

10. Unless otherwise specified, "respondent" shall mean TRENDnet, Inc., and its successors and assigns.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, other device, or an affiliate owned or controlled by respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

A. The extent to which respondent or its products or services maintain and protect:

1. The security of Covered Device Functionality;

2. The security, privacy, confidentiality, or integrity of any Covered Information; and

B. The extent to which a consumer can control the security of any Covered Information input into, stored on, captured with, accessed, or transmitted by a Covered Device.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this Order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks that could result in unauthorized access to or use of Covered Device Functionality, and (2) protect the security, confidentiality, and integrity of Covered Information, whether collected by respondent, or input into, stored on, captured with, accessed, or transmitted through a Covered Device. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device Functionality or Covered Information, including:

A. The designation of an employee or employees to coordinate and be accountable for the security program;

B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or use of Covered Device Functionality, and assessment of the sufficiency of any safeguards in place to control these risks;

C. The identification of material internal and external risks to the security, confidentiality, and integrity of Covered Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent's possession or is input into, stored on, captured with, accessed, or transmitted through a Covered

Device, and assessment of the sufficiency of any safeguards in place to control these risks;

D. At a minimum, the risk assessments required by Subparts B and C should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-party security vulnerability reports;

E. The design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Information is restricted consistent with a user's security settings;

F. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this Order, and requiring service providers, by contract, to establish and implement, and thereafter maintain, appropriate safeguards consistent with this Order; and

H. The evaluation and adjustment of the security program in light of the results of the testing and monitoring required by Subpart F, any material changes to the respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this Order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Covered Devices or other similar Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Covered Devices or other similar Internet-accessible consumer-grade devices; or a similarly qualified person or organization; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal

Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the Order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the Order for the biennial Assessments. Each Assessment shall:

A. Set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device Functionality or Covered Information;

C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this Order; and

D. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Device Functionality and the security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the Order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of TRENDnet, Inc.*, FTC File No. 1223090, Docket No. C-4426. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IV.

IT IS FURTHER ORDERED that respondent shall:

A. Notify Affected Consumers, clearly and prominently, that their Cameras had a flaw that allowed third parties to access their Live Feed Information without inputting authentication credentials, despite their security setting choices; and provide instructions on how to remove this flaw. Notification shall include, but not be limited to, each of the following means:

1. On or before ten (10) days after the date of service of this Order and for two (2) years after the date of service of this Order, posting of a notice on its website;

2. On or before ten (10) days after the date of service of this Order and for three (3) years after the date of service of this Order, informing Affected Consumers who complain or inquire about a Camera; and

3. On or before ten (10) days after the date of service of this Order and for three (3) years after the date of service of this Order, informing Affected Consumers who register, or who have registered, their Camera with respondent; and

B. Provide prompt and free support with clear and prominent contact information to help consumers update and/or uninstall a Camera. For two (2) years after the date of service of this Order, this support shall include toll-free, telephonic and electronic mail support.

V.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. For a period of five (5) years after the date of preparation of each Assessment required under Part III of this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Part III of this Order, for the compliance period covered by such Assessment;

B. Unless covered by V.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this Order, including but not limited to:

1. All advertisements, promotional materials, installation and user guides, and packaging containing any representations covered by this Order, as well as all materials used or relied upon in making or disseminating the representation; and

2. Any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this Order.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this Order to all (1) current and future subsidiaries, (2) current and future principals, officers, directors, and managers, (3) current and future employees, agents, and representatives having responsibilities relating to the subject matter of this Order, and (4) current and future manufacturers and service providers of the Covered Products. Respondent shall deliver this Order to such current subsidiaries, personnel, manufacturers, and service providers within thirty (30) days after service of this Order, and to such future subsidiaries, personnel, manufacturers, and service providers within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this section.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this Order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the Matter of TRENDnet, Inc.*, FTC File No. 1223090, Docket No. C-4426. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VIII.

IT IS FURTHER ORDERED that respondent within sixty (60) days after the date of service of this Order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this Order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

IX.

This Order will terminate on January 16, 2034, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the Order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this Order that terminates in fewer than twenty (20) years;

B. This Order's application to any respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: January 16, 2014

142 3156

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	)	**DOCKET NO. C-4587**
ASUSTeK Computer, Inc., a corporation.	)	

COMPLAINT

The Federal Trade Commission, having reason to believe that ASUSTeK Computer, Inc. ("respondent") has violated the provisions of the Federal Trade Commission Act, and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent ASUSTeK Computer, Inc. is a Taiwanese corporation with its principal office or place of business at 15, Li-Te Rd., Peitou, Taipei 11259, Taiwan.

2. The acts and practices of respondent as alleged in this complaint have been in or affecting commerce, as "commerce" is defined in Section 4 of the Federal Trade Commission Act.

RESPONDENT'S BUSINESS PRACTICES

3. Respondent ASUSTeK Computer, Inc. ("ASUS") is a hardware manufacturer that, among other things, sells routers, and related software and services, intended for consumer use. ASUS designs the software for its routers, controls U.S. marketing and advertising for its routers, including on websites targeting U.S. consumers, and is responsible for developing and distributing software updates to remediate security vulnerabilities and other flaws in routers sold to U.S. consumers. ASUS sells its routers in the United States through a wholly owned U.S. subsidiary, which distributes the routers for sale through third-party retailers, in stores and online, throughout the United States.

RESPONDENT'S ROUTERS AND "CLOUD" FEATURES

4. Routers forward data packets along a network. In addition to routing network traffic, consumer routers typically function as a hardware firewall for the local network, and act as the first line of defense in protecting consumer devices on the local network, such as computers, smartphones, internet-protocol ("IP") cameras, and other connected

appliances, against malicious incoming traffic from the internet. Respondent marketed its routers as including security features such as "SPI intrusion detection" and "DoS protection," advertised that its routers could "protect computers from any unauthorized access, hacking, and virus attacks" (*see* Exh. A, p. 1 of 2), and instructed consumers to "enable the [router's] firewall to protect your local network against attacks from hackers" (*see* Exh. A, p. 2 of 2).

5. Consumers set up and control the router's configuration settings, including its security-related settings, through a web-based graphical user interface (the "admin console"). In order to configure these settings, consumers must log in to the admin console with a username and password, which ASUS preset on all of its routers to the default username "admin" and password "admin" (*see* Exh. B). The admin console also provides a tool that ostensibly allows consumers to check whether the router is using the latest available firmware – the software that operates the router.

6. Many of respondent's routers include software features called AiCloud and AiDisk that allow consumers to wirelessly access and share files through their router. Depending on the model, respondent's routers that include these "cloud" features have a list price in the range of $69.99 to $219.99. As of March 2014, respondent had sold over 918,000 of these routers to U.S. consumers.

AICLOUD

7. In August 2012, ASUS introduced and began marketing a feature known as AiCloud on its routers. Respondent publicized AiCloud as a "private personal cloud for selective file sharing" that featured "indefinite storage and increased privacy" (*see* Exh. C, p. 1 of 6). In the following months, ASUS provided software updates for certain older router models to add the AiCloud feature, which respondent touted as "the most complete, accessible, and secure cloud platform" (*see* Exh. C, p. 2 of 6).

8. Described as "your secure space," AiCloud allows consumers to plug a USB storage device, such as an external hard drive, into the router, and then use web and mobile applications to access files on the storage device (*see* Exh. C, p. 3 of 6). For example, a consumer could save documents to the storage device using a desktop computer, and then later access those documents using a laptop, smartphone, or tablet. AiCloud also allows consumers to share specific files with others through a "secure URL," manage shared files, and revoke file access (*see* Exh. C, pp. 3-6 of 6).

Multiple Vulnerabilities

9. The AiCloud web and mobile applications require consumers to log in with the router's username and password (*see* Exh. D). However, the AiCloud web application included multiple vulnerabilities that would allow attackers to gain unauthorized access to consumers' files and router login credentials. In order to exploit these vulnerabilities, an attacker would only need to know the router's IP address – information that, as described in Paragraph 32, is easily discoverable.

10. First, attackers could exploit an authentication bypass vulnerability to access the consumer's AiCloud account without the consumer's login credentials. By sending a specific command, or simply entering a specific URL in a web browser, an attacker could bypass the AiCloud web application's authentication screen and gain unauthorized access to a consumer's files, even if the consumer had not designated any of these files for sharing.

11. Second, attackers could exploit a password disclosure vulnerability in the AiCloud web application to retrieve the consumer's router login credentials in clear, readable text. In addition to providing the attacker with access to the consumer's AiCloud account, attackers could also use these login credentials to gain unauthorized access to the router's configuration settings. For example, if a consumer had enabled the admin console's remote management feature, an attacker could use the login credentials to simply log into the consumer's admin account and modify any of the router's settings, including its firewall and other security settings. Even if this remote management feature was disabled, an attacker could use the credentials in conjunction with other well-known vulnerabilities that affected respondent's routers, such as the cross-site request forgery vulnerabilities described in Paragraphs 24-26, to force unauthorized changes to the router's security settings, placing the consumer's local network at risk.

Failure to Provide Timely Notice

12. Several individuals notified respondent about the AiCloud vulnerabilities in June 2013. Furthermore, in September 2013, a consumer complained to ASUS that his "entire life [was] hacked" due to the AiCloud vulnerabilities, and that he needed to obtain identity theft protection services as a result. Despite knowing about these serious vulnerabilities and their impact on respondent's customers, respondent failed to notify consumers about the vulnerabilities or advise them to take simple steps, such as disabling the AiCloud features, that would have mitigated the vulnerabilities.

13. Between July 2013 and September 2013, ASUS updated the firmware for affected routers in order to correct the AiCloud vulnerabilities. However, it was not until February 2014, eight months after respondent first learned of the vulnerabilities and after the events described in Paragraph 32, that respondent emailed registered customers notifying them that firmware updates addressing these and other security risks were available.

AIDISK

14. ASUS has offered another "cloud" feature on many of its routers called "AiDisk" since as early as 2009. Like AiCloud, AiDisk enables consumers to remotely access files on a USB storage device attached to the router, but does so through a file transfer protocol ("FTP") server. Despite the fact that FTP does not support transit encryption, since at least 2012 respondent has promoted AiDisk as a way to "safely secure and access your treasured data through your router" (*see* Exh. E). In addition to transferring files unencrypted, the AiDisk software included a number of other design flaws that placed consumers' sensitive personal information at risk.

Insecure Design

15. Consumers could set up an AiDisk FTP server in two ways. The first was through a set of menus called the "AiDisk wizard." During setup, the AiDisk wizard asks the consumer to "Decide how to share your folders," and presents three options: "limitless access rights," "limited access rights," and "admin rights." Prior to January 2014, the AiDisk wizard did not provide consumers with sufficient information to evaluate these options, and pre-selected the "limitless access rights" option for the consumer (*see* Exh. F, p. 1 of 2). If the consumer completed setup with this default option in place, the AiDisk wizard created an FTP server that would provide anyone on the internet who had the router's IP address with unauthenticated access to the consumer's USB storage device.

16. The second way consumers could set up an AiDisk FTP server was through a submenu in the admin console called "USB Application – FTP Share." The submenu did not provide consumers with any information regarding the default settings or the alternative settings that were available. If a consumer clicked on the option to "Enable FTP" (*see* Exh. G, p. 1 of 2), the software created an AiDisk FTP server that, by default, provided anyone on the internet who had the router's IP address with unauthenticated access to the consumer's USB storage device.

17. Neither set-up option provided any explanation that the default settings would provide anyone on the internet with unauthenticated access to all of the files saved on the consumer's USB storage device. And in both cases, search engines could index any of the files exposed by these unauthenticated FTP servers, making them easily searchable online.

18. If a consumer wanted to prevent unauthenticated access through the AiDisk wizard, the consumer needed to deviate from the default settings and select "limited access rights." The consumer would then be presented with the option to create login credentials for the FTP server. However, the AiDisk wizard recommended that the consumer choose weak login credentials, such as the preset username "Family" and password "Family" (*see* Exh. F, p. 2 of 2). In the alternative, the consumer could select "admin rights," which would apply the same login credentials for the FTP server that the consumer used to log in to the router's admin console. As described in Paragraphs 11 and 24, however, due to multiple password disclosure vulnerabilities, attackers could access these router login credentials in clear, readable text, undermining the protection provided by these credentials.

19. If a consumer wanted to prevent unauthenticated access through the "USB Application – FTP Share" submenu, the software provided no explanation or guidance as to how the consumer could change the default settings. The consumer would need to know to click on the "Share with account" option (*see* Exh. G, p. 1 of 2), which would allow the consumer to set up login credentials for the AiDisk FTP server. Confusingly, however, the software presented the consumer with a warning that implied that this option would expand, rather than restrict, access to the FTP server: "Enabling share with account enables multiple computers, with different access rights, to access the file resources. Are you sure you want to enable it?" (*see* Exh. G, p. 2 of 2). Through this misleading

warning, respondent discouraged consumers from taking steps that could have prevented unauthenticated access to their sensitive personal information.

Notice of Design Flaws and Failure to Mitigate

20. In June 2013, a security researcher publicly disclosed that, based on his research, more than 15,000 ASUS routers allowed for unauthenticated access to AiDisk FTP servers over the internet. In his public disclosure, the security researcher claimed that he had previously contacted respondent about this and other security issues. In November 2013, the security researcher again contacted respondent, warning that, based on his research, 25,000 ASUS routers now allowed for unauthenticated access to AiDisk FTP servers. The researcher suggested that respondent warn consumers about this risk during the AiDisk set up process. However, ASUS took no action at the time.

21. Two months later, in January 2014, several European media outlets published stories covering the security risks caused by the AiDisk default settings. At that time, a large European retailer requested that respondent update the AiDisk default settings. Although respondent had known about the security risks for months, it was only after this retailer's request that respondent took some steps to protect its customers. In response, ASUS began releasing updated firmware that changed the AiDisk wizard's default setting – for new set-ups – from "limitless access rights" to "limited access rights," and displayed a warning message if consumers selected "limitless access rights" that "any user can access your FTP service without authentication!" However, respondent did not notify consumers about the availability of this firmware update.

22. Moreover, the January 2014 firmware update did not change the insecure default settings for consumers who had already set up AiDisk. Respondent did not notify those consumers that they would need to complete the AiDisk wizard process again in order for the new defaults to apply, or would need to manually change the settings.

23. It was not until February 2014 – following the events described in Paragraph 32 – that respondent sent an email to registered customers notifying them that firmware updates addressing these security risks and other security vulnerabilities were available. Furthermore, it was not until February 21, 2014 that ASUS released a firmware update that would provide some protection to consumers who had previously set up AiDisk. This firmware update forced consumers' routers to turn off unauthenticated access to the AiDisk FTP server.

OTHER VULNERABILITIES

24. ASUS's router firmware and admin console have also been susceptible to a number of other well-known and reasonably foreseeable vulnerabilities – including multiple password disclosure, cross-site scripting, cross-site request forgery, and buffer overflow vulnerabilities – that attackers could exploit to gain unauthorized administrative control over consumers' routers.

25. For example, the admin console has been susceptible to pervasive cross-site request forgery ("CSRF") vulnerabilities that would allow an attacker to force malicious changes to any of the router's security settings (*e.g.*, disabling the firewall, enabling remote management, allowing unauthenticated access to an AiDisk server, or configuring the router to redirect the consumer to malicious websites) without the consumer's knowledge. Despite the serious consequences of these vulnerabilities, respondent did not perform pre-release testing for this class of vulnerabilities. Nor did respondent implement well-known, low-cost measures to protect against them, such as anti-CSRF tokens – unique values added to requests sent between a web application and a server that only the server can verify, allowing the server to reject forged requests sent by attackers.

26. Beginning in March 2013, respondent received multiple reports from security researchers regarding the CSRF vulnerabilities affecting respondent's routers. Despite these reports, respondent took no action to fix the vulnerabilities for at least a year, placing consumers' routers at risk of exploit. Indeed, in April 2015, a malware researcher discovered a large-scale, active CSRF exploit campaign that reconfigured vulnerable routers so that the attackers could control and redirect consumers' web traffic. This exploit campaign specifically targeted numerous ASUS router models.

FIRMWARE UPGRADE TOOL

27. The admin console includes a tool that ostensibly allows consumers to check whether their router is using the most current firmware ("firmware upgrade tool"). When consumers click on the "Check" button, the tool indicates that the "router is checking the ASUS server for the firmware update" (*see* Exh. H).

28. In order for the firmware upgrade tool to recognize the latest available firmware, ASUS must update a list of available firmware on its server. On several occasions, ASUS has failed to update this list. In July 2013, respondent received reports that the firmware upgrade tool was not recognizing the latest available firmware from both a product review journalist and by individuals calling into respondent's customer-support call center. Likewise, in February 2014, a security researcher notified respondent that the firmware upgrade tool did not recognize the latest available firmware, and detailed the reasons for the failure. In an internal email from that time, respondent acknowledged that, "if this list is not up to date when you use the check for update button in the [admin console,] the router doesn't find an update and states it is already up to date." Again, in October 2014 and January 2015, additional consumers reported to ASUS that the firmware upgrade tool still did not recognize the latest available firmware.

29. As a result, in many cases, respondent's firmware upgrade tool inaccurately notifies consumers that the "router's current firmware is the latest version" when, in fact, newer firmware with critical security updates is available.

RESPONDENT'S FAILURE TO REASONABLY SECURE ITS ROUTERS AND RELATED "CLOUD" FEATURES

30. Respondent has engaged in a number of practices that, taken together, failed to provide reasonable security in the design and maintenance of the software developed for its routers and related "cloud" features. Among other things, respondent failed to:

    a. perform security architecture and design reviews to ensure that the software is designed securely, including failing to:

        i. use readily-available secure protocols when designing features intended to provide consumers with access to their sensitive personal information. For example, respondent designed the AiDisk feature to use FTP rather than a protocol that supports transit encryption;

        ii. implement secure default settings or, at the least, provide sufficient information that would ensure that consumers did not unintentionally expose sensitive personal information;

        iii. prevent consumers from using weak default login credentials to protect critical security functions or sensitive personal information. For example, respondent allowed consumers to retain the weak default login credentials username "admin" and password "admin" for the admin console, and username "Family" and password "Family" for the AiDisk FTP server;

    b. perform reasonable and appropriate code review and testing of the software to verify that access to data is restricted consistent with a user's privacy and security settings;

    c. perform vulnerability and penetration testing of the software, including for well-known and reasonably foreseeable vulnerabilities that could be exploited to gain unauthorized access to consumers' sensitive personal information and local networks, such as authentication bypass, clear-text password disclosure, cross-site scripting, cross-site request forgery, and buffer overflow vulnerabilities;

    d. implement readily-available, low-cost protections against well-known and reasonably foreseeable vulnerabilities, as described in (c), such as input validation, anti-CSRF tokens, and session time-outs;

    e. maintain an adequate process for receiving and addressing security vulnerability reports from third parties such as security researchers and academics;

    f. perform sufficient analysis of reported vulnerabilities in order to correct or mitigate all reasonably detectable instances of a reported vulnerability, such as those elsewhere in the software or in future releases; and

    g. provide adequate notice to consumers regarding (i) known vulnerabilities or security risks, (ii) steps that consumers could take to mitigate such vulnerabilities

or risks, and (iii) the availability of software updates that would correct or mitigate the vulnerabilities or risks.

THOUSANDS OF ROUTERS COMPROMISED

31. Due to the failures described in Paragraphs 7-30, respondent has subjected its customers to a significant risk that their sensitive personal information and local networks will be subject to unauthorized access.

32. For example, on or before February 1, 2014, a group of hackers used readily available tools to locate the IP addresses of thousands of vulnerable ASUS routers. Exploiting the AiCloud vulnerabilities and AiDisk design flaws, the hackers gained unauthorized access to the attached USB storage devices of thousands of consumers and saved a text file on the storage devices warning these consumers that their routers were compromised: "This is an automated message being sent out to everyone effected [sic]. Your Asus router (and your documents) can be accessed by anyone in the world with an internet connection." The hackers then posted online a list of IP addresses for 12,937 vulnerable ASUS routers as well as the login credentials for 3,131 AiCloud accounts, further exposing these consumers to potential harm.

33. Numerous consumers reported having their routers compromised, based on their discovery of the text-file warning the hackers had saved to their attached USB storage devices. Some complained that a major search engine had indexed the files that the vulnerable routers had exposed, making them easily searchable online. Others claimed to be the victims of related identity theft. For example, one consumer claimed that identity thieves had gained unauthorized access to his USB storage device, which contained his family's sensitive personal information, including login credentials, social security numbers, dates of birth, and tax returns. According to the consumer, in March 2014, identity thieves used this information to make thousands of dollars of fraudulent charges to his financial accounts, requiring him to cancel accounts and place a fraud alert on his credit report. Moreover, the consumer claimed that he had attempted to upgrade his router's firmware on several occasions after he bought the device in December 2013, but that the firmware upgrade tool had erroneously indicated that his router was using the latest available firmware. Given the sensitivity of the stolen personal information, he and his family are at a continued risk of identity theft.

34. Even consumers who did not enable the AiCloud and AiDisk features have been at risk of harm due to numerous vulnerabilities in respondent's router firmware and admin console. As described in Paragraphs 24-26, attackers could exploit these vulnerabilities to gain unauthorized control over a consumer's router and modify its security settings without the consumer's knowledge.

THE IMPACT OF RESPONDENT'S FAILURES ON CONSUMERS

35. As demonstrated by the thousands of compromised ASUS routers, respondent's failure to employ reasonable security practices has subjected consumers to substantial injury. Unauthorized access to sensitive personal information stored on attached USB storage devices, such as financial information, medical information, and private photos and videos, could lead to identity theft, extortion, fraud, or other harm. Unauthorized access and control over the router could also lead to the compromise of other devices on the local network, such as computers, smartphones, IP cameras, or other connected appliances. Finally, such unauthorized access and control could allow an attacker to redirect a consumer seeking, for example, a legitimate financial site to a fraudulent site, where the consumer would unwittingly provide the attacker with sensitive financial information. Consumers had little, if any, reason to know that their sensitive personal information and local networks were at risk.

36. Respondent could have prevented or mitigated these risks through simple, low-cost measures. In several instances, respondent could have prevented consumer harm by simply informing consumers about security risks, and advising them to disable or update vulnerable software. In other cases, respondent could have protected against vulnerabilities by implementing well-known and low-cost protections, such as input validation, anti-CSRF tokens, and session time-outs, during the software design process. Finally, simply preventing consumers from using weak default login credentials would have greatly increased the security of consumers' routers.

ROUTER SECURITY MISREPRESENTATIONS
(Count 1)

37. As described in Paragraph 4, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its routers could protect consumers' local networks from attack.

38. In fact, as described in Paragraphs 11, 24-26, and 30, respondent did not take reasonable steps to ensure that its routers could protect consumers' local networks from attack. Therefore, the representation set forth in Paragraph 37 is false or misleading.

AICLOUD SECURITY MISREPRESENTATIONS
(Count 2)

39. As described in Paragraphs 7-8, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its AiCloud feature is a secure means for a consumer to access sensitive personal information.

40. In fact, as described in Paragraphs 9-13 and 30, respondent did not take reasonable steps to ensure that its AiCloud feature is a secure means for a consumer to access sensitive personal information. Therefore, the representation set forth in Paragraph 39 is false or misleading.

AIDISK SECURITY MISREPRESENTATIONS
(Count 3)

41. As described in Paragraph 14, respondent has represented, expressly or by implication, directly or indirectly, that it took reasonable steps to ensure that its AiDisk feature is a secure means for a consumer to access sensitive personal information.

42. In fact, as described in Paragraphs 14-23 and 30, respondent did not take reasonable steps to ensure that its AiDisk feature is a secure means for a consumer to access sensitive personal information. Therefore, the representation set forth in Paragraph 41 is false or misleading.

FIRMWARE UPGRADE TOOL MISREPRESENTATIONS
(Count 4)

43. As described in Paragraph 27, respondent has represented, expressly or by implication, that consumers can rely upon the firmware upgrade tool to indicate accurately whether their router is using the most current firmware.

44. In fact, as described in Paragraphs 28-29, consumers cannot rely upon the firmware upgrade tool to indicate accurately whether their router is using the most current firmware. Therefore, the representation set forth in Paragraph 43 is false or misleading.

UNFAIR SECURITY PRACTICES
(Count 5)

45. As set forth in Paragraphs 4-36, respondent has failed to take reasonable steps to secure the software for its routers, which respondent offered to consumers for the purpose of protecting their local networks and accessing sensitive personal information. Respondent's actions caused or are likely to cause substantial injury to consumers in the United States that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice is an unfair act or practice.

46. The acts and practices of respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this eighteenth day of July, 2016, has issued this complaint against respondent.

By the Commission.

Donald S. Clark
Secretary

142 3156

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: **Edith Ramirez, Chairwoman**
Maureen K. Ohlhausen
Terrell McSweeny

In the Matter of	**DECISION AND ORDER**
ASUSTeK Computer Inc., **a corporation.**	**DOCKET NO. C-4587**

DECISION

The Federal Trade Commission ("Commission") initiated an investigation of certain acts and practices of the Respondent named above in the caption. The Commission's Bureau of Consumer Protection ("BCP") prepared and furnished to Respondent a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondent with violation of the Federal Trade Commission Act.

Respondent and BCP thereafter executed an Agreement Containing Consent Order ("Consent Agreement"). The Consent Agreement includes: 1) statements by Respondent that it neither admits nor denies any of the allegations in the Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, it admits the facts necessary to establish jurisdiction; and 2) waivers and other provisions as required by the Commission's Rules.

The Commission considered the matter and determined that it had reason to believe that Respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days, and duly considered the comments filed thereafter by interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34. Now, in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

1. Respondent ASUSTeK Computer, Inc., is a Taiwanese corporation with its principal office or place of business at 15, Li-Te Rd., Peitou, Taipei 11259, Taiwan.

2. The Commission has jurisdiction over the subject matter of this proceeding and over the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. Unless otherwise specified, "respondent" shall mean ASUSTeK Computer, Inc., corporation, and its subsidiaries and divisions in the United States, and successors and assigns.

2. "Clear(ly) and conspicuous(ly)" means that a required disclosure is difficult to miss (i.e., easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:

   A. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication, even if the representation requiring the disclosure is made in only one means.

   B. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

   C. An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

   D. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.

   E. The disclosure must use diction and syntax understandable to ordinary consumers.

   F. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

   G. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

3. "Commerce" shall mean commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation, as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

4. "Covered Device" shall mean (a) any router, or device for which the primary purpose is connecting other client devices to a network, developed by respondent, directly or indirectly, that is marketed to consumers in the United States and (b) the software used to access, operate, manage, or configure such router or other device subject to part (a) of this definition, including, but not limited to, the firmware, web or mobile applications, and any related online services, that are advertised, developed, branded, or provided by respondent, directly or indirectly, for use with, or as compatible with, the router or other device.

5. "Covered Information" shall mean any individually-identifiable information from or about an individual consumer collected by respondent through a Covered Device or input into, stored on, captured with, accessed, or transmitted through a Covered Device, including but not limited to (a) a first and last name; (b) a home or other physical address; (c) an email address or other online contact information; (d) a telephone number; (e) a Social Security number; (f) financial information; (g) an authentication credential, such as a username or password; (h) photo, video, or audio files; (i) the contents of any communication, the names of any websites sought, or the information entered into any website.

6. "Default Settings" shall mean any configuration option on a Covered Device that respondent preselects, presets, or prefills for the consumer.

7. "Software Update" shall mean any update designed to address a Security Flaw.

8. "Security Flaw" is a software vulnerability or design flaw in a Covered Device that creates a material risk of (a) unauthorized access to or modification of any Covered Device, (b) the unintentional exposure by a consumer of Covered Information, or (c) the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of Covered Information.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, in or affecting commerce, must not misrepresent in any manner, expressly or by implication:

A. The extent to which respondent or its products or services maintain and protect:

1. The security of any Covered Device;

2. The security, privacy, confidentiality, or integrity of any Covered Information;

B. The extent to which a consumer can use a Covered Device to secure a network; and

C. The extent to which a Covered Device is using up-to-date software.

II.

IT IS FURTHER ORDERED that respondent must, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing Covered Devices, and (2) protect the privacy, security, confidentiality, and integrity of Covered Information. Such program, the content and implementation of which must be fully documented in writing, must contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device's function or the Covered Information, including:

A. The designation of an employee or employees to coordinate and be accountable for the security program;

B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or unauthorized modification of a Covered Device, and assessment of the sufficiency of any safeguards in place to control these risks;

C. The identification of material internal and external risks to the privacy, security, confidentiality, and integrity of Covered Information that could result in the unintentional exposure of such information by consumers or the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks;

D. At a minimum, the risk assessments required by Subparts B and C must include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development, and research; (3) secure software design, development, and testing, including for Default Settings; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

E. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, including through reasonable and appropriate software security testing techniques, such as (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Devices and Covered Information is restricted consistent with a user's security settings;

F. Regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards consistent with this order; and

H. The evaluation and adjustment of respondent's security program in light of the results of the testing and monitoring required by Subpart F, any material changes to respondent's operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of the security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent must obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments must be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Internet-accessible consumer-grade devices; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. The reporting period for the Assessments must cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment must:

A. Set forth the specific controls and procedures that respondent has implemented and maintained during the reporting period;

B. Explain how such safeguards are appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the Covered Device's function or the Covered Information;

C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. Certify that respondent's security program is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Devices and the privacy, security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

Each Assessment must be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent must provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments must be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In re ASUSTek Computer Inc.*, FTC File No. 142 3156.

IV.

IT IS FURTHER ORDERED that respondent must:

A. Notify consumers, Clearly and Conspicuously, when a Software Update is available, or when respondent is aware of reasonable steps that a consumer could take to mitigate a Security Flaw. The notice must explain how to install the Software Update, or otherwise mitigate the Security Flaw, and the risks to the consumer's Covered Device or Covered Information if the consumer chooses not to install the available Software Update or take the recommended steps to mitigate the Security Flaw. Notice must be provided through at least each of the following means:

1. Posting of a Clear and Conspicuous notice on at least the primary, consumer-facing website of respondent and, to the extent feasible, on the user interface of any Covered Device that is affected;

2. Directly informing consumers who register, or who have registered, a Covered Device with respondent, by email, text message, push notification, or another similar method of providing notifications directly to consumers; and

3. Informing consumers who contact respondent to complain or inquire about any aspect of the Covered Device they have purchased.

B. Provide consumers with an opportunity to register an email address, phone number, device, or other information during the initial setup or configuration of a Covered Device, in order to receive the security notifications required by this Part. The consumer's registration of such information must not be dependent upon or defaulted to an agreement to receive non-security related notifications or any other communications, such as advertising. Notwithstanding this requirement, respondent may provide an option for consumers to opt-out of receiving such security-related notifications.

V.

IT IS FURTHER ORDERED that respondent must maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. For a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent's compliance with Part III of this order, for the compliance period covered by such Assessment;

B. Unless covered by V.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:

1. All advertisements, promotional materials, installation and user guides, and packaging containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation;

2. All notifications required by Part IV of this order; and

3. Any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent's compliance with this order.

VI.

IT IS FURTHER ORDERED that respondent must deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this order. Respondent must deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such

position or responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery must be at least ten (10) days prior to the change in structure.

VII.

IT IS FURTHER ORDERED that respondent must notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. *Provided, however*, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent must notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part must be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: *In re ASUSTek Computer Inc.*, FTC File No. 142 3156.

VIII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, must file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it must submit additional true and accurate written reports.

IX.

This order will terminate on July 18, 2036, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in fewer than twenty (20) years;

B. This order's application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: July 18, 2016

Patents in the New Media

Douglas A. Miro, Esq.
Amster Rothstein & Ebenstein, LLP (Moderator)

Charles Macedo, Esq.
Amster Rothstein & Ebenstein, LLP

Richard P. Zemsky
Chief Operating Officer, AIMeCast, LLC

Finjan, Inc. v. Blue Coat Sys.

United States Court of Appeals for the Federal Circuit

January 10, 2018, Decided

2016-2520

Reporter
879 F.3d 1299 *; 2018 U.S. App. LEXIS 601 **; 125 U.S.P.Q.2D (BNA) 1282 ***; 2018 WL 341882

FINJAN, INC., Plaintiff-Appellee v. BLUE COAT SYSTEMS, INC., Defendant-Appellant

Prior History: [1]** Appeal from the United States District Court for the Northern District of California in No. 5:13-cv-03999-BLF, Judge Beth Labson Freeman.

Finjan, Inc. v. Blue Coat Sys., 2016 U.S. Dist. LEXIS 93267 (N.D. Cal., July 18, 2016)

Disposition: AFFIRMED-IN-PART, REVERSED-IN-PART, AND REMANDED.

Core Terms

patent, infringement, Downloadable, profile, users, royalty, damages, policies, cache, scans, web, Computing, district court, functionality, identifies, commands, gateway, Proxy, apportionment, suspicious, files, argues, royalty rate, non-infringement, categories, patentee, linking, virus, substantial evidence, abstract idea

Case Summary

Overview
HOLDINGS: [1]-In a patent infringement case involving four computer security patents, the district court did not err in its subject matter eligibility determination under *35 U.S.C.S. § 101* because the claims did not recite a mere result, but instead recited specific steps that accomplished the desired result; [2]-While substantial evidence supported the jury's finding of infringement of two patents, the accused infringer was entitled to JMOL of non-infringement for a third patent because the accused products did not perform the claimed "policy index" limitation; [3]-With respect to damages, award was supported with respect to two of the infringed patents, reversed for the non-infringed patent, and remanded for the fourth patent because patentee failed to apportion damages to the infringing functionality and the $8-per-user royalty rate was unsupported by substantial evidence.

Outcome
Decision affirmed-in-part, reversed-in-part, and remanded to the district court for further consideration of the damages issue as to one patent.

LexisNexis® Headnotes

Patent Law > Jurisdiction & Review > Standards of Review > De Novo Review

Patent Law > Subject Matter

HN1[] **Standards of Review, De Novo Review**

District court decisions regarding patent subject matter eligibility are reviewed de novo.

Patent Law > Subject Matter

HN2[] **Patent Law, Subject Matter**

35 U.S.C.S. § 101 provides that a patent may be obtained for any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof. *35 U.S.C.S. § 101*. The Supreme Court has long recognized, however, that *§ 101* implicitly excludes laws of nature, natural phenomena, and abstract ideas from the realm of patent-eligible subject matter, as monopolization of these basic tools of scientific and technological work would stifle the very innovation that the patent system

aims to promote.

Patent Law > ... > Utility Patents > Process Patents > Computer Software & Mental Steps

Patent Law > Subject Matter

HN3 **Process Patents, Computer Software & Mental Steps**

The Supreme Court has instructed us to use a two-step framework to distinguish patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts. At the first step, the court determines whether the claims at issue are "directed to" a patent-ineligible concept. If they are, the court then considers the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application. This is the search for an "inventive concept"—something sufficient to ensure that the claim amounts to significantly more than the abstract idea itself. In cases involving software innovations, the step one inquiry often turns on whether the claims focus on the specific asserted improvement in computer capabilities or, instead, on a process that qualifies as an abstract idea for which computers are invoked merely as a tool.

Patent Law > ... > Utility Patents > Process Patents > Computer Software & Mental Steps

HN4 **Process Patents, Computer Software & Mental Steps**

For purposes of a subject matter eligibility analysis under *35 U.S.C.S. § 101*, the United States Court of Appeals for the Federal Circuit has concluded that, by itself, virus screening is well-known and constitutes an abstract idea. The Federal Circuit has also found that performing the virus scan on an intermediary computer—so as to ensure that files are scanned before they can reach a user's computer—is a perfectly conventional approach and is also abstract.

Patent Law > ... > Utility Patents > Process Patents > Computer Software & Mental Steps

HN5 **Process Patents, Computer Software & Mental Steps**

For purposes of a subject matter eligibility analysis under *35 U.S.C.S. § 101*, software-based innovations can make non-abstract improvements to computer technology and be deemed patent-eligible subject matter at step one of the Alice framework.

Patent Law > Subject Matter

HN6 **Patent Law, Subject Matter**

It is a foundational patent law principle that a result, even an innovative result, is not itself patentable. That is, patents are granted for the discovery or invention of some practicable method or means of producing a beneficial result or effect, and not for the result or effect itself.

Civil Procedure > Trials > Judgment as Matter of Law

Patent Law > Jurisdiction & Review > Standards of Review > Abuse of Discretion

Patent Law > Jurisdiction & Review > Standards of Review > De Novo Review

Civil Procedure > Judgments > Relief From Judgments > Motions for New Trials

HN7 **Trials, Judgment as Matter of Law**

In patent cases, the United States Court of Appeals for the Federal Circuit reviews denials of motions for judgment as a matter of law (JMOL) de novo and motions for new trial for abuse of discretion.

Civil Procedure > Trials > Judgment as Matter of Law > Postverdict Judgment

Patent Law > Infringement Actions > Claim Interpretation

Patent Law > Jurisdiction & Review > Standards of Review > Substantial Evidence

HN8 **Judgment as Matter of Law, Postverdict**

Judgment

In a patent infringement case, it is too late at the judgment as a matter of law (JMOL) post-verdict stage to argue for or adopt a new and more detailed interpretation of patent claim language and test the jury verdict by that new and more detailed interpretation. Under such circumstances, the question for the trial court is limited to whether substantial evidence supports the jury's verdict under the issued construction.

Patent Law > Remedies > Damages > Measure of Damages

Patent Law > ... > Damages > Patentholder Losses > Reasonable Royalties

HN9[] **Damages, Measure of Damages**

In a patent infringement case, *35 U.S.C.S. § 284* limits damages to those adequate to compensate for the infringement. Two categories of compensation for infringement are the patentee's lost profits and the reasonable royalty he would have received through arms-length bargaining. A reasonable royalty seeks to compensate the patentee for its lost opportunity to obtain a reasonable royalty that the infringer would have been willing to pay if it had been barred from infringing.

Patent Law > Remedies > Damages > Measure of Damages

Patent Law > ... > Damages > Patentholder Losses > Reasonable Royalties

HN10[] **Damages, Measure of Damages**

With respect to patent infringement damages, when the accused technology does not make up the whole of the accused product, apportionment is required. The ultimate combination of royalty base and royalty rate must reflect the value attributable to the infringing features of the product, and no more. That is, no matter what the form of the royalty, a patentee must take care to seek only those damages attributable to the infringing features. In such cases, the patentee must give evidence tending to separate or apportion the infringer's profits and the patentee's damages between the patented feature and the unpatented features, and such evidence must be reliable and tangible, and not conjectural or speculative. The patent holder has the burden of proving damages by a preponderance of the evidence.

Patent Law > Remedies > Damages > Measure of Damages

Patent Law > ... > Damages > Patentholder Losses > Reasonable Royalties

HN11[] **Damages, Measure of Damages**

With respect to patent infringement damages, the smallest salable unit principle directs that in any case involving multi-component products, patentees may not calculate damages based on sales of the entire product, as opposed to the smallest salable patent-practicing unit, without showing that the demand for the entire product is attributable to the patented feature. With respect to reasonable royalty awards, the essential requirement is that the ultimate reasonable royalty award must be based on the incremental value that the patented invention adds to the end product. If the smallest salable unit—or smallest identifiable technical component—contains non-infringing features, additional apportionment is still required. Whether viewed as valuable, important, or even essential, the patented feature must be separated.

Patent Law > ... > Damages > Patentholder Losses > Reasonable Royalties

HN12[] **Patentholder Losses, Reasonable Royalties**

With respect to patent infringement damages, while any reasonable royalty analysis necessarily involves an element of approximation and uncertainty, a trier of fact must have some factual basis for a determination of a reasonable royalty. Alleging a loose or vague comparability between different technologies or licenses does not suffice. Also, there must be a basis in fact to associate the royalty rates used in prior licenses to a particular hypothetical negotiation at issue in the case.

Patent Law > ... > Damages > Patentholder Losses > Reasonable Royalties

HN13[] **Patentholder Losses, Reasonable**

Royalties

Ordinarily, the district court must award damages in an amount no less than a reasonable royalty when patent infringement is found, unless the patent holder has waived the right to damages based on alternate theories.

Patent Law > ... > Damages > Patentholder Losses > Reasonable Royalties

HN14[] **Patentholder Losses, Reasonable Royalties**

The direction in *35 U.S.C.S. § 284* to award damages "in no event less than a reasonable royalty" does not mean that the patentee need not support the award with reliable evidence. A jury may not award more than is supported by the record.

Counsel: PAUL J. ANDRE, Kramer Levin Naftalis & Frankel LLP, Menlo Park, CA, argued for plaintiff-appellee. Also represented by JAMES R. HANNAH, LISA KOBIALKA.

MARK A. LEMLEY, Durie Tangri LLP, San Francisco, CA, argued for defendant-appellant. Also represented by SONALI DEEKSHA MAITRA, SONAL NARESH MEHTA, CLEMENT ROBERTS; OLIVIA M. KIM, EDWARD POPLAWSKI, Wilson, Sonsini, Goodrich & Rosati, P.C., Los Angeles, CA.

Judges: Before DYK, LINN, and HUGHES, Circuit Judges..

Opinion by: DYK

Opinion

[*1284] [*1302]** DYK, *Circuit Judge*.

A jury found Blue Coat Systems, Inc. ("Blue Coat") liable for infringement of four patents owned by Finjan, Inc. ("Finjan") and awarded approximately $39.5 million in reasonable royalty damages. After trial, the district court concluded that the '844 patent was patent-eligible under *35 U.S.C. § 101* and denied Blue Coat's post-trial motions for judgment as a matter of law ("JMOL") and a new trial. Blue Coat appeals.

We find no error in the district court's subject matter eligibility determination as to the '844 patent and agree that substantial evidence supports the jury's **[**2]** finding of infringement of the '844 and '731 patents. However, we conclude that Blue Coat was entitled to JMOL of non-infringement for the '968 patent because the accused products do not perform the claimed "policy index" limitation. On appeal, Blue Coat does not challenge the verdict of infringement for the '633 patent.

With respect to damages, we affirm the award with respect to the '731 and '633 patents. We vacate the damages award for the '968 patent, as there was no infringement. With respect to the '844 patent, we agree with Blue Coat that Finjan failed to apportion damages to the infringing functionality and that the $8-per-user royalty rate was unsupported by substantial evidence.

We therefore affirm-in-part, reverse-in-part, and remand to the district court for further consideration of the damages issue as to the '844 patent.

BACKGROUND

On August 28, 2013, Finjan brought suit against Blue Coat in the Northern District of California for infringement of patents owned by Finjan and directed to identifying and protecting against malware. Four of those patents are at issue on appeal. Claims 1, 7, 11, 14, and 41 of U.S. Patent No. 6,154,844 ("the '844 patent") recite a system and method for providing computer security by attaching a security profile to a downloadable. Claims 1 and 17 of U.S. Patent No. 7,418,731 ("the '731 patent") recite a system and method **[**3]** for providing computer security at a network gateway by comparing security profiles associated with requested files to the security policies of requesting users. Claim 1 of U.S. Patent No. 6,965,968 ("the '968 patent") recites a "policy-based cache manager" that indicates the allowability of cached files under a plurality of user security policies. Claim 14 of U.S Patent No. 7,647,633 ("the '633 patent") relates to a system and method for using "mobile **[***1285]** code runtime monitoring" to protect against malicious downloadables.

After a trial, the jury found that Blue Coat infringed these four patents and awarded Finjan approximately $39.5 million for Blue Coat's infringement: $24 million for the '844 patent, $6 million for the '731 patent, $7.75 million for the '968 patent, and $1,666,700 for the '633 patent. After a bench trial, the district court concluded that the '844 patent is directed to patent-eligible subject matter under *35 U.S.C. § 101*.

Thereafter, the district court denied Blue Coat's motions for judgment as a matter of law and a new trial, concluding that Finjan had provided substantial evidence to support each finding of infringement and the damages award. Blue Coat appeals the district court's rulings on subject matter eligibility of the '844 patent; infringement of the '844, '731, and '968 patents; and damages for the '844, '731, '968, and '633 patents. We have jurisdiction pursuant to **[**4]** 28 U.S.C. § 1295(a)(1).

[*1303] DISCUSSION

I. Subject Matter Eligibility of the '844 Patent

We first address subject matter eligibility with respect to the '844 patent. HN1[] We review the district court's decision de novo. McRO, Inc. v. Bandai Namco Games Am. Inc., 837 F.3d 1299, 1311 (Fed. Cir. 2016).

HN2[] *Section 101* provides that a patent may be obtained for "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." *35 U.S.C. § 101*. The Supreme Court has long recognized, however, that *§ 101* implicitly excludes "laws of nature, natural phenomena, and abstract ideas" from the realm of patent-eligible subject matter, as monopolization of these "basic tools of scientific and technological work" would stifle the very innovation that the patent system aims to promote. Alice Corp. v. CLS Bank Int'l, 134 S. Ct. 2347, 2354, 82 L. Ed. 2d 296, 189 L. Ed. 2d 296 (2014) (quoting Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576, 133 S. Ct. 2107, 2116, 186 L. Ed. 2d 124 (2013)); *see also* Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 132 S. Ct. 1289, 1294-97, 182 L. Ed. 2d 321 (2012); Diamond v. Diehr, 450 U.S. 175, 185, 101 S. Ct. 1048, 67 L. Ed. 2d 155 (1981).

HN3[] The Supreme Court has instructed us to use a two-step framework to "distinguish[] patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts." Alice, 134 S. Ct. at 2355. At the first step, we determine whether the claims at issue are "directed to" a patent-ineligible concept. *Id.* If they are, we then "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature **[**5]** of the claim' into a patent-eligible application." *Id.* (quoting Mayo, 132 S. Ct. at 1298). This is the search for an "inventive concept"—something sufficient to ensure that the claim amounts to "significantly more" than the abstract idea itself. *Id.* (quoting Mayo, 132 S.Ct. at 1294).

Starting at step one, we must first examine the '844 patent's "claimed advance" to determine whether the claims are directed to an abstract idea. Affinity Labs of Tex., LLC v. DIRECTV, LLC, 838 F.3d 1253, 1257 (Fed. Cir. 2016). In cases involving software innovations, this inquiry often turns on whether the claims focus on "the specific asserted improvement in computer capabilities . . . or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1335-36 (Fed. Cir. 2016).

The '844 patent is directed to a method of providing computer security by scanning a downloadable and attaching the results of that scan to the downloadable itself in the form of a "security profile." Claim 1 of the '844 patent, which the district court found representative for *§ 101* purposes, reads:

1. A method comprising:
receiving by an inspector a Downloadable;
generating by the inspector a first Downloadable security profile that identifies suspicious code in the received Downloadable; and

linking by the inspector the first Downloadable security profile to the Downloadable **[**6]** before a web server makes the Downloadable available to web clients.

[*1286]** '844 patent, col. 11 ll. 11-21. At claim construction, the parties agreed that "Downloadable" should be construed to mean "an executable application program, which is downloaded from a source computer and run on the destination computer." **[*1304]** Additionally, the district court construed "Downloadable security profile that identifies suspicious code in the received Downloadable" to mean "a profile that identifies code in the received Downloadable that performs hostile or potentially hostile operations."

We determined in Intellectual Ventures I LLC v. Symantec Corp., 838 F.3d 1307, 1319 (Fed. Cir. 2016), that HN4[] "[b]y itself, virus screening is well-known and constitutes an abstract idea." We also found that performing the virus scan on an intermediary computer—so as to ensure that files are scanned before they can reach a user's computer—is a "perfectly conventional" approach and is also abstract. Id. at 1321.

Here the claimed method does a good deal more.

Claim 1 of the '844 patent scans a downloadable and attaches the virus scan results to the downloadable in the form of a newly generated file: a "security profile that identifies suspicious code in the received Downloadable." The district court's claim construction decision emphasizes that this **[**7]** "identif[y] suspicious code" limitation can only be satisfied if the security profile includes "details about the suspicious code in the received downloadable, such as . . . 'all potentially hostile or suspicious code operations that may be attempted by the Downloadable.'" *Finjan, Inc. v. Blue Coat Sys., Inc., No. 13-CV-03999-BLF, 2014 U.S. Dist. LEXIS 149077, 2014 WL 5361976, at *9 (N.D. Cal. Oct. 20, 2014)*. The security profile must include the information about *potentially* hostile operations produced by a "behavior-based" virus scan. This operation is distinguished from traditional, "code-matching" virus scans that are limited to recognizing the presence of previously-identified viruses, typically by comparing the code in a downloadable to a database of known suspicious code. The question, then, is whether this behavior-based virus scan in the '844 patent constitutes an improvement in computer functionality. We think it does.

The "behavior-based" approach to virus scanning was pioneered by Finjan and is disclosed in the '844 patent's specification. In contrast to traditional "code-matching" systems, which simply look for the presence of known viruses, "behavior-based" scans can analyze a downloadable's code and determine whether it performs potentially dangerous or unwanted operations—such as **[**8]** renaming or deleting files. Because security profiles communicate the granular information about potentially suspicious code made available by behavior-based scans, they can be used to protect against previously unknown viruses as well as "obfuscated code"—known viruses that have been cosmetically modified to avoid detection by code-matching virus scans.

The security profile approach also enables more flexible and nuanced virus filtering. After an inspector generates a security profile for a downloadable, a user's computer can determine whether to access that downloadable by reviewing its security profile according to the rules in whatever "security *policy*" is associated with the user. Administrators can easily tailor access by applying different security policies to different users or types of users. And having the security profile include information about particular potential threats enables administrators to craft security policies with highly granular rules and to alter those security policies in response to evolving threats.

Our cases confirm that ***HN5***[↑] software-based innovations can make "non-abstract improvements to computer technology" and be deemed patent-eligible subject matter **[**9]** at step 1. *Enfish, 822 F.3d at 1335-36*. In *Enfish*, for instance, the court determined that claims related to a database architecture that used a new, self-referential logical **[*1305]** table were non-abstract because they focused on "an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity." *Id. at 1336*. Indeed, the self-referential database found patent eligible in *Enfish* did more than allow computers to perform familiar tasks with greater speed and efficiency; it actually permitted users to launch and construct databases in a new way. While deployment of a traditional relational database involved "extensive modeling and configuration of the various tables and relationships in advance of launching the database," *Enfish*'s self-referential database could be launched "with no or only minimal column definitions" and **[***1287]** configured and adapted "on-the-fly." *Id. at 1333*.

Similarly, the method of claim 1 employs a new kind of file that enables a computer security system to do things it could not do before. The security profile approach allows access to be tailored for different users and ensures that threats are identified before a file reaches a user's computer. The fact that **[**10]** the security profile "identifies suspicious code" allows the system to accumulate and utilize newly available, behavior-based information about potential threats. The asserted claims are therefore directed to a non-abstract improvement in computer functionality, rather than the abstract idea of computer security writ large.

Even accepting that the claims are directed to a new idea, Blue Coat argues that they remain abstract because they do not sufficiently describe how to implement that idea. To support this argument, Blue Coat points to *Apple, Inc. v. Ameranth, Inc.*, where we invalidated claims related to a computer system that can generate a second menu from a first menu based on a selection of items on the first menu. *842 F.3d 1229, 1240-41 (Fed. Cir. 2016)*. In that case, we held that the patents were directed to an abstract idea because they "d[id] not claim a particular way of programming or designing the software . . . but instead merely claim the resulting systems." *Id. at 1241*. Blue Coat also relies on

Affinity Labs, where we held that a claim related to wirelessly communicating regional broadcast content to an out-of-region recipient was abstract and patent ineligible because there was nothing in the claim "directed to *how* to implement **[**11]** [the idea]. Rather, the claim is drawn to the idea itself." *838 F.3d at 1258*. And Blue Coat also notes that, in *Intellectual Ventures*, we found claims directed to email filtering to be abstract and patent ineligible when there is "no restriction on how the result is accomplished . . . [and] [t]he mechanism . . . is not described." *838 F.3d 1307, 1316 (Fed. Cir. 2016)* (quoting *Internet Patents Corp. v. Active Network, Inc., 790 F.3d 1343, 1348 (Fed. Cir. 2015)*).

Apple, *Affinity Labs*, and other similar cases hearken back to ***HN6***[↑] a foundational patent law principle: that a result, even an innovative result, is not itself patentable. *See* *Corning v. Burden, 56 U.S. 252, 268, 14 L. Ed. 683 (1853)* (explaining that patents are granted "for the discovery or invention of some practicable method or means of producing a beneficial result or effect . . . and not for the result or effect itself"); *O'Reilly v. Morse, 56 U.S. 62, 112-113, 14 L. Ed. 601 (1853)* (invalidating a claim that purported to cover all uses of electromagnetism for which "the result is the making or printing intelligible characters, signs, or letters at a distance" as "too broad, and not warranted by law").

Here, the claims recite more than a mere result. Instead, they recite specific steps—generating a security profile that identifies suspicious code and linking it to a downloadable—that accomplish the desired result. Moreover, there is no contention that the only thing disclosed is the **[**12]** **[*1306]** result and not an inventive arrangement for accomplishing the result. There is no need to set forth a further inventive concept for implementing the invention. The idea is non-abstract and there is no need to proceed to step two of *Alice*.

II. Infringement

At trial, the jury found that Blue Coat's products infringed the '844, '731, and '968 patents. The district court denied Blue Coat's post-trial motions for judgment as a matter of law and a new trial, finding that Finjan had provided substantial evidence to support each finding of infringement and that the jury verdict was not against the weight of the evidence. ***HN7***[↑] We review denials of motions for JMOL de novo and motions for new trial for abuse of discretion. *Revolution Eyewear, Inc. v. Aspex Eyewear, Inc., 563 F.3d 1358, 1370-71 (Fed. Cir. 2009)*.

A. '844 Patent

Blue Coat first argues that the district court should have granted JMOL of non-infringement as to the asserted claims in the '844 patent because substantial evidence did not support the jury verdict. Specifically, Blue Coat contends that the asserted claims, requiring linking a security profile to a downloadable "before a web server makes the Downloadable available to web clients," can only be infringed by a server-side product that evaluates content before it is published to the Internet in the first place. **[**13]** Blue Coat's product, WebPulse, is a cloud-based service that provides information about downloadables to a customer's network gateway in order to help the network gateway determine whether a particular **[***1288]** downloadable can be accessed by a specific end user. Because WebPulse only evaluates downloadables that are already publicly available on the Internet, Blue Coat argues that it does not infringe.

Blue Coat made no request for a claim construction that would require linking the security profile to the downloadable before the downloadable is placed on the Internet. Blue Coat cannot raise the claim construction issue for the first time in post-trial motions: ***HN8***[↑] "it is too late at the JMOL stage to argue for or adopt a new and more detailed interpretation of the claim language and test the jury verdict by that new and more detailed interpretation." *Hewlett-Packard Co. v. Mustek Sys., Inc., 340 F.3d 1314, 1321 (Fed. Cir. 2003)*. Under such circumstances, "the question for the trial court is limited to whether substantial evidence supports the jury's verdict under the issued construction." *Wi-Lan, Inc. v. Apple, Inc., 811 F.3d 455, 465 (Fed. Cir. 2016)*. Here, the claim, as construed by the district court, requires "linking by the inspector the first Downloadable security profile to the Downloadable before [a/the] non-network gateway **[**14]** web server make[s] the Downloadable available to web clients." '844 patent, col. 11 ll. 18-20; J.A. 25. The jury was instructed to apply this construction.

It was reasonable for the jury to interpret "web clients" in this context to refer to the specific web clients protected by the claimed system. Likewise, the limitation requiring that linking occur before a downloadable is "ma[de] . . . available to web clients" could reasonably be understood to require that linking occur at some point before users are *permitted to access* that downloadable—but not necessarily before the downloadable is made available on the Internet. Blue Coat concedes that, at the time a security profile is linked, the "particular web client cannot yet ***receive*** the downloadable—but the ***web server*** has made it available . . . ." Reply Br. 9. Given the undisputed

evidence that WebPulse links security profiles to downloadables before downloadables can be received by **[*1307]** users of the service, we find that the '844 infringement verdict was supported by substantial evidence.

B. '731 Patent

We next consider Blue Coat's claim that it was entitled to JMOL of non-infringement as to the asserted claims of the '731 patent. The '731 patent is directed to a computer gateway that protects a **[**15]** private intranet from malicious software embedded in webpages on the public Internet.[1] The claimed gateway operates by scanning potentially malicious files and creating "security profiles" that each comprise "a list of computer commands that the file is programmed to perform." '731 patent, col. 4 ll. 47-48. Claim 17 further specifies that the security profile include "a list of at least one computer command that the retrieved file is programmed to perform." '731 patent, col. 13 ll. 7-8. Once these security profiles have been generated, they can be compared with the security policy associated with a given user in order to decide whether the file should be provided to that user.

Blue Coat argues that the '731 patent was not infringed as a matter of law because the "security profiles" created by the accused product do not contain the requisite "list of computer commands." Because Blue Coat did not request a construction of the "list of commands" term, we apply the ordinary meaning. We find that substantial evidence supports the jury's finding of infringement.

At trial, Finjan presented evidence demonstrating that the accused product creates a new file called "cookie2" each time it scans an incoming file for potential malware. Cookie2 comprises a set of fields, each field representing various characteristics about the downloadable file. Fields 78-80 of Cookie2 represent **[***1289]** certain commands and show whether those commands—such as eval(), **[**17]** unescape(), and document.write()—appear in the incoming file. In fields 78-80, an integer represents the number of times each command appears. Finjan's expert, Dr. Mitzenmacher, testified that the data contained in fields 78-80 "is clearly a list of computer commands." J.A. 40383.

Blue Coat argues that this is not enough and that the "list of commands" limitation cannot be satisfied by "an ***identifier*** of a ***type*** of command the system should watch for." Appellant Br. 34. But the claim language simply requires that the security profile contain "a list of computer commands that a corresponding one of the incoming files is programmed to perform." It does not mandate any particular representation of that information—much less require that the commands be listed in the form of executable code. Dr. Mitzenmacher **[*1308]** testified at trial that the integers in fields 78-80 are "clearly a list of computer commands" because "those numbers determine whether or not those commands are in the security profile." J.A. 40383-84. He also notes that "there are many ways of representing a list [of computer commands], including the way it is represented here." J.A. 40384. Substantial evidence supports the jury's implied **[**18]** finding that the "list of commands" limitation is satisfied by the integers in Fields 78-80 of Cookie2, and the patent is infringed.

C. '968 Patent

Blue Coat also argues that it was entitled to JMOL of non-infringement with respect to the '968 patent because Finjan failed to introduce substantial evidence that the accused products implement the claimed "policy index." We agree.

The '968 patent is directed to a "policy-based" cache manager that can efficiently manage cached content according to a plurality of security policies. The patentee agrees that a "policy" is a rule or set of rules that

---

[1] Claim 1 of the '731 patent reads:

> 1. A computer gateway for an intranet of comput-ers, comprising:
>
> a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files, wherein each of the security profiles comprises a list of computer commands that a corresponding one of the incoming files is programmed to perform;
>
> a file cache for storing files that have been scanned by the scanner for future access, wherein each of the stored files is indexed by a file identifier; and
>
> a security profile cache for storing the security profiles **[**16]** derived by the scanner, wherein each of the security profiles is indexed in the security profile cache by a file identifier associated with a corresponding file stored in the file cache; and
>
> a security policy cache for storing security policies for intranet computers within the intranet, the security policies each including a list of restrictions for files that are transmitted to a corresponding subset of the intranet computers.
>
> '731 patent, col. 11 ll. 35-55.

determines whether a piece of content can be accessed by a user. Different policies can apply to different users, and the decision of whether to let a user access content is made by comparing the content's security profile with the policy governing the user's access. Thus, the policy based cache manager in the '968 patent is a data structure that keeps track of whether content is permitted under various policies. Claim 1, the sole asserted claim, is reproduced below, with key language underlined:

1. A policy-based cache manager, comprising:

> a memory storing a cache of digital content, a plurality of policies, and a policy index to the cache **[**19]** contents, the policy index including entries that relate cache content and policies by indicating cache content that is known to be allowable relative to a given policy, for each of a plurality of policies;
> a content scanner, communicatively coupled with said memory, for scanning a digital content received, to derive a corresponding content profile; and
>
> a content evaluator, communicatively coupled with said memory, for determining whether a given digital content is allowable relative to a given policy, based on the content profile, the results of which are saved as entries in the policy index.

'968 patent col. 9 ll. 47-62. At claim construction, the parties stipulated that "policy index" means "a data structure indicating allowability of cached content relative to a plurality of policies." The jury was instructed to apply this construction. Once again, we test the jury's infringement verdict based on this claim language and claim construction. *Hewlett-Packard Co., 340 F.3d at 1320-21*.

Trial testimony demonstrated that the accused product, Proxy SG, is a gateway between an intranet of computers and the Internet at large. Every time a user requests a file, Proxy SG will analyze that file and determine whether access is permitted under the **[**20]** user's security policy. As Proxy SG evaluates a file, it can cache the results of individual rules *within* a policy and use that information to speed up the process of making an ultimate policy decision. Early in its analysis, for instance, Proxy SG can check the "category" of the file and then determine whether the user's policy has any rules related to the "category" field. Proxy SG can then store "the evaluations of the parts of the rules that deal with this category field . . . . So you don't have to reevaluate those conditions again." J.A. 40327-28. As Finjan's expert expressly acknowledged, however, Proxy **[*1309]** SG does not save final decisions about whether content can be accessed by users subject to a given policy. It simply stores the evaluation of each individual **[***1290]** rule that goes into making an ultimate policy decision. This is not what the claim language requires. The policy index claimed in the '968 patent must store the "results" of a content evaluator's determination of "whether a given digital content is allowable relative to a given policy."

At summary judgment, the district court agreed that this claim language requires the policy index to store final allowability determinations and noted **[**21]** that "Defendant's argument would likely prevail if all policies consist of multiple rules or conditions." *Finjan, Inc. v. Blue Coat Sys., Inc., No. 13-CV-03999-BLF, 2015 U.S. Dist. LEXIS 74566, 2015 WL 3630000, at *9 (N.D. Cal. June 2, 2015)*. The court nevertheless declined to grant summary judgement because "the '968 patent specifically provides that a policy can be just one rule." *Id.* If Proxy SG saved the results of applying each rule that makes up a one-rule policy, it would be saving final allowability determinations for a plurality of policies and thus infringing. The district court therefore gave Finjan the opportunity to prove at trial that "the Proxy SG policy cache contains a number of condition evaluations, each of which is determinative of whether a file is allowable relative to one of a plurality of single condition policies." *Id.*

At trial, Finjan made no such showing. There was no evidence indicating that the condition determinations stored by Proxy SG are final allowability decisions for users governed by single-rule policies. Indeed, Finjan's expert acknowledged that Proxy SG never saves final allowability determinations and must instead re-evaluate the allowability of content each time it is requested. It is therefore clear that the jury's infringement verdict **[**22]** was not supported by substantial evidence.

Because Finjan failed to present evidence that the accused product ever stores final allowability determinations, Blue Coat was entitled to JMOL of non-infringement.

III. Damages

We now turn to Blue Coat's damages arguments with respect to the '844, '731, and '633 patents. The starting point is ***HN9***[↑] *35 U.S.C. § 284*, which limits damages to those "adequate to compensate for the infringement." Two categories of compensation for infringement are

the patentee's lost profits and the "reasonable royalty he would have received through arms-length bargaining." *Lucent Techs., Inc. v. Gateway, Inc., 580 F.3d 1301, 1324 (Fed. Cir. 2009)*.

The only measure of damages at issue in this case is a reasonable royalty, which "seeks to compensate the patentee . . . for its lost opportunity to obtain a reasonable royalty that the infringer would have been willing to pay if it had been barred from infringing." *AstraZeneca AB v. Apotex Corp., 782 F.3d 1324, 1334 (Fed. Cir. 2015)* (citing *Lucent Techs., 580 F.3d at 1325*).

A. '844 Patent

Blue Coat first argues that, in calculating a royalty base, Finjan failed to apportion damages to the infringing functionality. We agree.

HN10[↑] When the accused technology does not make up the whole of the accused product, apportionment is required. "[T]he ultimate combination of royalty base and royalty rate must reflect the value attributable to the infringing features **[**23]** of the product, and no more." *Ericsson, Inc. v. D-Link Sys., Inc., 773 F.3d 1201, 1226 (Fed. Cir. 2014)*; *see also Mentor Graphics v. EVE-USA, 870 F.3d 1298, 1299 (Fed. **[*1310]** Cir. 2017)* (order denying rehearing en banc) ("[W]here an infringing product is a multi-component product with patented and unpatented components, apportionment is required."); *VirnetX, Inc. v. Cisco Sys., Inc., 767 F.3d 1308, 1326 (Fed. Cir. 2014)* ("No matter what the form of the royalty, a patentee must take care to seek only those damages attributable to the infringing features."). In such cases, the patentee must "give evidence tending to separate or apportion the [infringer]'s profits and the patentee's damages between the patented feature and the unpatented features, and such evidence must be reliable and tangible, and not conjectural or speculative." *Garretson v. Clark, 111 U.S. 120, 121, 4 S. Ct. 291, 28 L. Ed. 371, 1884 Dec. Comm'r Pat. 206 (1884)*. Finjan, as the present patent holder, had the burden of proving damages by a preponderance of the evidence.

WebPulse, the infringing product, is a cloud-based system that associates URLs with over eighty different categories, including pornography, gambling, shopping, social networking, and "suspicious"—which is a category meant to identify potential malware. WebPulse is not sold by itself. Rather, other **[***1291]** Blue Coat products, like Proxy SG, use WebPulse's category information to make allowability determinations about URLs that end users are trying to access.

DRTR, which stands **[**24]** for "dynamic real-time rating engine," is the part of WebPulse responsible for analyzing URLs that have not already been categorized. DRTR performs both infringing and non-infringing functions. When a user requests access to a URL that is not already in the WebPulse database—a brand new website, for instance—DRTR will analyze the content, assign a category or categories, and collect metadata about the site for further use. As part of that analysis, DRTR will examine the URL for malicious or suspicious code, create a kind of "security profile" highlighting that information, and then "attach" the security profile to the given URL. This infringes the '844 patent. But the DRTR analysis also evaluates whether the URL fits into categories ranging from pornography to news. These additional categories are unrelated to DRTR's malware identification function but are still valuable for companies trying to, say, prevent employees from using social media while on the job. DRTR also collects metadata about the URL for Blue Coat's later use. In other words, all of the infringing functionality occurs in DRTR, but some DRTR functions infringe and some do not.

At trial, Finjan attempted to tie the royalty base **[**25]** to the incremental value of the infringement by multiplying WebPulse's total number of users by the percentage of web traffic that passes through DRTR, the WebPulse component that performs the infringing method. DRTR processes roughly 4% of WebPulse's total web requests, so Finjan established a royalty base by multiplying the 75 million worldwide WebPulse users by 4%. Although DRTR also performs the non-infringing functions described above, Finjan did not perform any further apportionment on the royalty base.

Finjan argues that apportionment to DRTR is adequate because DRTR is the "smallest, identifiable technical component" tied to the footprint of the invention. Appellee Br. 49-50. This argument, which draws from this court's precedent regarding apportionment to the "smallest salable patent-practicing unit" of an infringing product, does not help Finjan. ***HN11***[↑] The smallest salable unit principle directs that "in any case involving multi-component products, patentees may not calculate damages based on sales of the entire product, as opposed to the smallest salable patent-practicing unit, without showing that the **[*1311]** demand for the entire product is attributable to the patented feature." *LaserDynamics, Inc. v. Quanta Comput., Inc., 694 F.3d 51, 67-68 (Fed. Cir. 2012)*. The **[**26]** entire market

value rule is not at issue in this case, however, and the fact that Finjan has established a royalty base based on the "smallest, identifiable technical component" does not insulate them from the "essential requirement" that the "ultimate reasonable royalty award must be based on the incremental value that the patented invention adds to the end product." *Ericsson, 773 F.3d at 1226*. As we noted in *VirnetX*, if the smallest salable unit—or smallest identifiable technical component—contains non-infringing features, additional apportionment is still required. *VirnetX, 767 F.3d at 1327* (rejecting a jury instruction that "mistakenly suggest[ed] that when the smallest salable unit is used as the royalty base, there is necessarily no further constraint on the selection of the base").

Finjan further defends its apportionment methodology by asserting that it demonstrated that "many of these other categories were unimportant." Appellee Br. 51. But the claimed unimportance of particular categories (e.g. "Macy's and shopping") does not speak to the overall importance of identifying categories unrelated to malware. Malware detection is undoubtedly an important driver of DRTR's (and WebPulse's) value. At trial, for instance, Dr. Layne-Farrar pointed **[**27]** to an internal Blue Coat email stating that "[t]oday the main value of [Web-Filter and WebPulse] centers around zero-day malware protection." J.A. 40571. She also referenced a 2012 public-facing document entitled "Five reasons to choose Blue Coat," which gave "negative-day defense: stop malware at the source" as reason number two. J.A. 40572-73. But it is evident that Blue Coat's customers also value WebPulse's ability to identify and filter other categories of content. A Blue Coat whitepaper discussed at trial prominently advertises the fact that WebPulse provides "the granular category control that businesses need to implement acceptable Internet use policies." J.A. 53136. And Finjan's expert used an example about a company that wanted to bar access to certain sites categorized as "gambling." "Whether 'viewed as valuable, important, or **[***1292]** even essential,' the patented feature must be separated." *VirnetX, 767 F.3d at 1329* (quoting *LaserDynamics, 694 F.3d at 68*).

Because DRTR is itself a multi-component software engine that includes non-infringing features, the percent-age of web traffic handled by DRTR is not a proxy for the incremental value of the patented technology to WebPulse as a whole. Further apportionment was required to reflect the value **[**28]** of the patented technology compared to the value of the unpatented elements.

Blue Coat also identifies a second error in Finjan's reasonable royalty calculation. To arrive at a lump sum reasonable royalty payment for infringement of the '844 patent, Finjan simply multiplied the royalty base by an $8-per-user royalty rate. Blue Coat contends that there is no basis for the $8-per-user rate.

We agree with Blue Coat that the $8-per-user royalty rate employed in Finjan's analysis was unsupported by substantial evidence. There is no evidence that Finjan ever actually used or proposed an $8-per-user fee in any comparable license or negotiation. Rather, the $8-per-user fee is based on testimony from Finjan's Vice President of IP Licensing, Ivan Chaperot, that the current "starting point" in licensing negotiations is an "8 to 16 percent royalty rate or something that is consistent with that . . . like $8 per user fee." J.A. 40409. Mr. Chaperot further testified that the 8-16% figure was based on a 2008 **[*1312]** verdict obtained by Finjan against Secure Computing. On this basis, Finjan's counsel urged the jury to use an $8-per-user royalty rate for the hypothetical negotiation because "that's what Finjan would have **[**29]** asked for at the time." J.A. 41654.

HN12[↑] While any reasonable royalty analysis "necessarily involves an element of approximation and uncertainty, a trier of fact must have some factual basis for a determination of a reasonable royalty." *Unisplay, S.A. v. Am. Elec. Sign Co., 69 F.3d 512, 517 (Fed. Cir. 1995)*. Mr. Chaperot's testimony that an $8-per-user fee is "consistent with" the 8-16% royalty rate established in *Secure Computing* is insufficient. There is no evidence to support Mr. Chaperot's conclusory statement that an 8-16% royalty rate would correspond to an $8-per-user fee, and Finjan fails to adequately tie the facts of *Secure Computing* to the facts in this case. *See LaserDynamics, 694 F.3d at 79* ("[A]lleging a loose or vague comparability between different technologies or licenses does not suffice.").

Secure Computing did not involve the '844 patent, and there is no evidence showing that the patents that were at issue are economically or technologically comparable. Finjan's evidence on this point is limited to the fact that that the infringing products in *Secure Computing* were also in the computer security field and that Secure Computing was a competitor of Blue Coat in 2008. This surface similarity is far too general to be the basis for a reasonable royalty calculation. In any case, Mr. Chaperot's **[**30]** testimony that an 8-16% royalty rate would be the *current starting point* in licensing negotiations says little about what the parties would

have proposed or agreed to in a hypothetical arm's length negotiation in 2008. And Finjan's evidence of a $14-34 *software* user fee is not indicative of how much the parties would have paid to license a patent. *See* Uniloc USA, Inc. v. Microsoft Corp., 632 F.3d 1292, 1317 (Fed. Cir. 2011) ("[T]here must be a basis in fact to associate the royalty rates used in prior licenses to the particular hypothetical negotiation at issue in the case."). In short, the $8-per-user fee appears to have been plucked from thin air and, as such, cannot be the basis for a reasonable royalty calculation.

While it is clear that Finjan failed to present a damages case that can support the jury's verdict, reversal of JMOL could result in a situation in which Finjan receives no compensation for Blue Coat's infringement of the '844 patent. **HN13**[↑] Ordinarily, "the district court must award damages in an amount no less than a reasonable royalty" when infringement is found, Dow Chem. Co. v. Mee Indus., Inc., 341 F.3d 1370, 1381 (Fed. Cir. 2003); *see* Riles v. Shell Expl. & Prod. Co., 298 F.3d 1302, 1313 (Fed. Cir. 2002), unless the patent holder has waived the right to damages based on alternate theories, Promega Corp. v. Life Tech. Corp., 875 F.3d 651, 660 (Fed. Cir. 2017). We therefore remand to the district court to determine **[**31]** whether Finjan has waived the right to establish reasonable royalty damages under a new theory and whether to order a new trial on damages.

B. '731 and '633 Patents

For the '731 and '633 patents, Finjan's expert did apportion the revenues comprising the royalty base between infringing and non- **[***1293]** infringing functionality of Proxy SG. Blue Coat argues that the apportionment was insufficient. We disagree.

Finjan's expert, Dr. Layne-Farrar, based her apportionment analysis for the '731 and '633 patents on an architectural diagram prepared by Blue Coat. The diagram is entitled "Secure Web Gateway: Functions" and shows twenty-four boxes representing different parts of the Secure **[*1313]** Web Gateway system. Dr. Layne-Farrar assumed that each box represented one top level function and that each function was equally valuable. Thus, because one function infringed the '633 patent, and three infringed the '731 patent, she used a 1/24th apportionment for the '633 patent and a 3/24th apportionment for the '731 patent.

Blue Coat argues that there was no evidence to support Dr. Layne-Farrar's assumption that each box represents a "function" and that each function should be treated as equally valuable. But at trial, Dr. Layne-Farrar testified that her assumption was based on Blue Coat's own diagram, which **[**32]** is entitled "Secure Web Gateway: Functions", as well as her discussions with Mr. Medovic, a Finjan technical expert who explained the use of architectural diagrams and identified certain components within the diagram that did and did not infringe. Dr. Layne-Farrar also testified that she relied on the deposition of a Blue Coat engineer, in which the engineer stated that the diagram in question represents the full scope of Secure Web Gateway functionality. Based on this evidence, Dr. Layne-Farrar based her analysis on the twenty-four "functions" identified in the Blue Coat diagram and considered each function equally valuable.

Blue Coat notes that Dr. Layne-Farrar's conclusions conflict with testimony from Mr. Shoenfeld, Blue Coat's Senior VP of Products, stating that each box in the diagram can "have many, many things behind [it] . . . so there's no equal weighing of these [boxes] . . . ." *See* J.A. 40756. But the existence of conflicting testimony does not mean the damages award is unsupported by substantial evidence. The jury was entitled to believe the patentee's expert. The jury's damages awards for infringement of the '731 and '633 patents were based on substantial evidence.[2]

CONCLUSION

For the foregoing **[**33]** reasons, we reverse the denial of JMOL of non-infringement with respect to the '968 patent and remand to the district court to determine the issue of damages with respect to the '844 patent. We affirm in all other respects.

---

[2] Blue Coat also argues that the damages award was flawed because the jury awarded damages in excess of the estimates offered by Finjan's damages expert. Indeed, Finjan's damages expert gave a range of $2,979,805 to $3,973,073 for infringement of the '731 patent and a range of $833,350 to $1,111,133 for infringement of the '633 patent, JA 40623, but the jury awarded $6,000,000 for the '731 patent and $1,666,700 for the '633 patent, J.A. 125. We agree with Blue Coat that **HN14**[↑] the statute's direction to award damages "in no event less than a reasonable royalty" does not mean that the patentee need not support the award with reliable evidence. 35 U.S.C. § 284. A jury may not award more than is supported by the record, but here the record contains evidence that the expert's estimates were conservative and that the underlying evidence could support a higher award. J.A. 40619-20, 40656.

AFFIRMED-IN-PART, REVERSED-IN-PART, AND REMANDED.

COSTS

Each party shall bear its own costs.

Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.

United States Court of Appeals for the Federal Circuit

January 25, 2018, Decided

2016-2684, 2017-1922

Reporter
880 F.3d 1356 *; 2018 U.S. App. LEXIS 1931 **; 125 U.S.P.Q.2D (BNA) 1436 ***; 2018 WL 542672

CORE WIRELESS LICENSING S.A.R.L., Plaintiff-Appellee v. LG ELECTRONICS, INC., LG ELECTRONICS MOBILECOMM U.S.A., INC., Defendants-Appellants

Subsequent History: As Amended January 25, 2018.

Prior History: [1]** Appeals from the United States District Court for the Eastern District of Texas in Nos. 2:14-cv-00911-JRG-RSP, 2:14-cv-00912-JRG-SP, Judge J. Rodney Gilstrap.

Core Wireless Licensing S.a.r.l. v. LG Elecs., Inc., 2016 U.S. Dist. LEXIS 122745 (E.D. Tex., Sept. 12, 2016)
Core Wireless Licensing S.a.r.l. v. LG Elecs., Inc., 2016 U.S. Dist. LEXIS 35663 (E.D. Tex., Mar. 20, 2016)
Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc., 2016 U.S. Dist. LEXIS 112425 (E.D. Tex., Aug. 23, 2016)

Disposition: AFFIRMED.

Core Terms

display, patent, user, window, unlaunched, launch, menu, applications, screen, specification, functionality, invention, infringement, district court, devices, computing, anticipation, navigation, terms, asserted claim, abstract idea, matter of law, eligible, selectable, embodiment, improved, prior art, interfaces, invalidity, patentee

Case Summary

Overview

HOLDINGS: [1]-The record supported the district court's decision denying summary judgment to a patent holder's competitor on its claims that claims 8 and 9 of U.S. Patent No. 8,713,476 and claims 11 and 13 of U.S. Patent No. 8,434,020, which disclosed improved display interfaces, particularly for electronic devices with small screens like mobile telephones, were invalid under *35 U.S.C.S. § 101* because they were directed to an abstract idea; [2]-The district court did not err when it denied the competitor's motion for judgment as a matter of law on its claim that the claims in question were invalid under *35 U.S.C.S. § 102* because they were anticipated by prior art, or when it entered judgment confirming a jury's verdict that products the competitor sold infringed both patents; [3]-The claims in question were patentable because they recited a specific improvement over prior systems.

Outcome
Judgment affirmed.

LexisNexis® Headnotes

Patent Law > Claims & Specifications > Claims > Claim Language

Patent Law > Infringement Actions > Claim Interpretation > Scope of Claim

HN1[] **Claims, Claim Language**

When parties present a fundamental dispute regarding the scope of a term in a patent's claim, it is the court's duty to resolve it.

Civil Procedure > ... > Summary Judgment > Entitlement as Matter of Law > Appropriateness

Patent Law > Jurisdiction & Review > Standards of Review

Civil Procedure > Trials > Judgment as Matter of Law

Civil Procedure > Appeals > Standards of Review > De Novo Review

Civil Procedure > Appeals > Summary Judgment Review > Standards of Review

HN2[] Entitlement as Matter of Law, Appropriateness

For patent appeals, the United States Court of Appeals for the Federal Circuit applies the law of the regional circuit to issues not specific to patent law. The United States Court of Appeals for the Fifth Circuit reviews motions for summary judgment and motions for judgment as matter of law de novo. The Fifth Circuit views all evidence in a light most favorable to the verdict and will reverse a jury's verdict only if the evidence points so overwhelmingly in favor of one party that reasonable jurors could not arrive at any contrary conclusion.

Business & Corporate Compliance > ... > Patent Law > Infringement Actions > Infringing Acts

Patent Law > Jurisdiction & Review > Standards of Review > De Novo Review

Patent Law > Utility Requirement > Fact & Law Issues

Patent Law > Anticipation & Novelty > Fact & Law Issues

Patent Law > Jurisdiction & Review > Standards of Review > Substantial Evidence

HN3[] Infringement Actions, Infringing Acts

The ultimate determination of patent eligibility under *35 U.S.C.S. § 101* is an issue of law the United States Court of Appeals for the Federal Circuit reviews de novo. Anticipation and infringement are both questions of fact that are reviewed for substantial evidence when tried to a jury.

Patent Law > Utility Requirement > Proof of Utility

Patent Law > Jurisdiction & Review > Standards of Review

HN4[] Utility Requirement, Proof of Utility

Anyone who invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent. *35 U.S.C.S. § 101*. Because patent protection does not extend to claims that monopolize the building blocks of human ingenuity, claims directed to laws of nature, natural phenomena, and abstract ideas are not patent eligible. The United States Supreme Court instructs courts to distinguish between claims that claim patent ineligible subject matter and those that integrate the building blocks into something more. First, the United States Court of Appeals for the Federal Circuit determines whether the claims at issue are directed to a patent-ineligible concept. If so, the Federal Circuit examines the elements of the claim to determine whether it contains an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application. If claims are directed to a patent-eligible concept, they satisfy *§ 101* and the Federal Circuit need not proceed to the second step.

Patent Law > ... > Utility Patents > Process Patents > Computer Software & Mental Steps

Patent Law > Utility Requirement > Proof of Utility

Patent Law > Jurisdiction & Review > Standards of Review

HN5[] Process Patents, Computer Software & Mental Steps

At step one of an analysis under *35 U.S.C.S. § 101* to determine if a product or process is patentable, the United States Court of Appeals for the Federal Circuit must articulate what the claims are directed to with enough specificity to ensure the step-one inquiry is meaningful. Although there is difficulty inherent in delineating the contours of an abstract idea, the court must be mindful that all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas. The Federal Circuit also asks whether the claims are directed to a specific improvement in the capabilities of computing devices, or, instead, a process that qualifies as an

abstract idea for which computers are invoked merely as a tool.

Evidence > Burdens of Proof > Burden Shifting

Patent Law > Infringement Actions > Burdens of Proof

Patent Law > ... > Defenses > Patent Invalidity > Presumption of Validity

Evidence > Burdens of Proof > Clear & Convincing Proof

HN6 **Burdens of Proof, Burden Shifting**

A patent is presumed valid, and the burden of establishing invalidity of a claim rests on the party asserting invalidity by clear and convincing evidence. *35 U.S.C.S. § 282*. An alleged infringer asserting a defense of invalidity also has the initial burden of going forward with evidence to support its invalidity allegation. Once that evidence has been presented, the burden of going forward shifts to the patentee to present contrary evidence and argument. Ultimately, however, the outcome of an alleged infringer's invalidity defense at trial depends on whether the alleged infringer has carried its burden of persuasion to prove by clear and convincing evidence that the patent is invalid. Because the burden rests with the alleged infringer to present clear and convincing evidence supporting a finding of invalidity, granting judgment as a matter of law for the party carrying the burden of proof is generally reserved for extreme cases, such as when the opposing party's witness makes a key admission.

Patent Law > Jurisdiction & Review > Standards of Review > Clearly Erroneous Review

Patent Law > Infringement Actions > Claim Interpretation > Fact & Law Issues

Patent Law > Jurisdiction & Review > Standards of Review > De Novo Review

HN7 **Standards of Review, Clearly Erroneous Review**

The ultimate issue of the proper construction of a patent's claim should be treated as a question of law, which the United States Court of Appeals for the Federal Circuit reviews de novo. Any subsidiary factual findings related to claim construction are reviewed under the clearly erroneous standard. In construing a patent's claims, the Federal Circuit considers the words of the claims themselves, the specification, the prosecution history, and if necessary, any relevant extrinsic evidence. When a district court reviews only evidence intrinsic to a patent (the patent's claims and specifications, along with the patent's prosecution history), the judge's determination will amount solely to a determination of law.

Patent Law > Infringement Actions > Prosecution History Estoppel > Abandonment & Amendment

Patent Law > Jurisdiction & Review > Standards of Review

HN8 **Prosecution History Estoppel, Abandonment & Amendment**

The doctrine of prosecution disclaimer precludes patentees from recapturing the full scope of a claim term only when the patentee clearly and unmistakably disavows a certain meaning in order to obtain the patent. When an alleged disclaimer is ambiguous or amenable to multiple reasonable interpretations, the United States Court of Appeals for the Federal Circuit declines to find prosecution disclaimer.

Counsel: BENJAMIN T. WANG, Russ August & Kabat, Los Angeles, CA, argued for plaintiff-appellee. Also represented by MARC AARON FENSTER, ADAM S. HOFFMAN, REZA MIRZAIE; KAYVAN B. NOROOZI, Noroozi PC, Santa Monica, CA.

CARTER GLASGOW PHILLIPS, Sidley Austin LLP, Washington, DC, argued for defendants-appellants. Also represented by DANIEL HAY, RYAN C. MORRIS, ANNA MAYERGOYZ WEINBERG; PETER H. KANG, Palo Alto, CA; JAMES SUH, LG Electronics Inc., Seoul, Korea.

Judges: Before MOORE, O'MALLEY, and WALLACH, Circuit Judges. Opinion for the court filed by Circuit Judge MOORE. Opinion concurring-in-part and dissenting-in-part filed by Circuit Judge WALLACH.

Opinion by: MOORE

Opinion

[*1438] [*1359]** MOORE, *Circuit Judge*.

LG Electronics, Inc. ("LG") appeals the United States District Court for the Eastern District of Texas' decisions (1) denying summary judgment that claims 8 and 9 of U.S. Patent No. 8,713,476 ("'476 patent") and claims 11 and 13 of U.S. Patent No. 8,434,020 ("'020 patent") are directed to patent ineligible subject matter under *35 U.S.C. § 101*; (2) denying judgment as matter of law that U.S. Patent No. 6,415,164 ("Blanchard") anticipates the asserted claims under *35 U.S.C. § 102*; and (3) denying judgment as **[**2]** a matter of law that the claims are not infringed. For the reasons discussed below, we affirm.

BACKGROUND

The '476 and '020 patents disclose improved display interfaces, particularly for electronic devices with small screens like mobile telephones. '020 patent[1] at 1:14-24. The improved interfaces allow a user to more quickly access desired data stored in, and functions of applications included in, the electronic devices. *Id.* at 2:20-44. An application summary window displays "a limited list of common functions and commonly accessed stored data which itself can be reached directly from the main menu listing some or all applications." *Id.* at 2:55-59. The application summary window can be reached in two steps: "first, launch a main view which shows various applications; then, launch the appropriate summary window for the application of interest." *Id.* at 2:61-64. The patents explain that the disclosed application summary window "is far faster and easier than conventional navigation approaches," particularly for devices with small screens. *Id.* at 2:64-65.

Core Wireless Licensing S.A.R.L. ("Core Wireless") sued LG, alleging LG infringed dependent claims 8 and 9 of the '476 patent and dependent claims 11 and 13 of the '020 patent. Claims 8 **[**3]** and 9 of the '476 patent depend from claim 1, which recites (emphases added):

> 1. A computing device comprising a display screen, the computing device being configured to display on the screen a menu listing one or more applications, and additionally being configured to display on the screen an application summary that can be *reached directly* from the menu, wherein the application summary displays a limited list of data offered within the one or more applications, each of the data in the list being selectable to launch the respective application and enable the selected data to be seen within the respective application, and wherein the application summary is displayed while the one or more applications are in an *unlaunched state*.

[*1360] Claims 11 and 13 of the '020 patent depend from claim 1, which recites (emphases added):

> 1. A computing device comprising a display screen, the computing device being configured to display on the screen a main menu listing at least a first application, and additionally being configured to display on the screen an application summary window that can be *reached directly* from the main menu, wherein the application summary window displays a limited list of at least one function offered **[**4]** within the first application, each function in the list being selectable to launch the first application and initiate the selected function, and wherein the application summary window is displayed **[***1439]** while the application is in an *unlaunched state*.

LG moved for summary judgment of invalidity of the asserted claims under *35 U.S.C. § 101*, which the court denied. The district court found claim 1 of the '476 patent representative for the purposes of evaluating patent eligibility. It held that the claims are not directed to an abstract idea because, even crediting LG's characterization of the claims as directed to "displaying an application summary window while the application is in an unlaunched state," the concepts of "application," "summary window," and "unlaunched state" are specific to devices like computers and cell phones. J.A. 9561. The court explained "LG identifie[d] no analog to these concepts outside the context of such devices." *Id.* It further noted even "if claim 1 were directed to an abstract idea, it would still be patent eligible at least because it passes the machine-or-transformation test." J.A. 9562.

The case proceeded to trial, and the district court, after hearing initial testimony, determined **[**5]** "an *O2 Micro* situation" existed with respect to the claim terms "unlaunched state" and "reached directly," and afforded both sides an opportunity to argue constructions of these terms. J.A. 10277-78; *see O2 Micro Int'l Ltd. v.*

[1] The '476 and '020 patent specifications are effectively identical. Unless otherwise specified, citations to the '020 patent refer to disclosures in both patents.

Beyond Innovation Tech. Co., 521 F.3d 1351, 1362 (Fed. Cir. 2008) (***HN1***[↑] "When the parties present a fundamental dispute regarding the scope of a claim term, it is the court's duty to resolve it."). The district court ruled that "unlaunched state" means "not displayed" and "reached directly" means "reached without an intervening step."

The jury found all asserted claims infringed and not invalid. LG moved for judgment as matter of law of noninfringement, arguing in part that a correct construction of "unlaunched state" means "not running" and that under this construction, no reasonable jury could have found infringement. LG also argued that the "reached directly" limitation required user interaction with the main menu, and no reasonable jury could have found infringement under such a construction. The district court declined to revisit claim construction, noting LG did not preserve its claim construction arguments in a *Rule 50(a)* motion. The district court further denied LG's motion for judgment as a matter of law of noninfringement based on the court's adopted **[**6]** constructions because evidence was presented at trial from which the jury reasonably could have found that the application summary window in the accused devices could be reached directly from the main menu.

The district court also denied LG's motion for judgment of a matter of law of anticipation by Blanchard. Although Core Wireless elected not to call an expert to testify in rebuttal to LG's validity expert, the district court noted that the jury was not required to credit LG's expert testimony and concluded "LG failed to overcome the presumption of validity accorded to the '476 and '020 Patents by clear and convincing evidence." J.A. 18.

[*1361] LG timely appeals. We have jurisdiction under *28 U.S.C. § 1295(a)(1)*.[2]

DISCUSSION

[2] Concern remains regarding whether we have jurisdiction to review the appeal of validity and infringement determinations while damages remains unresolved and will be the subject of a future jury trial. This is particularly true where, as here, no judgment under *Rule 54(b)* or otherwise has ever been entered. This panel, however, is bound by the determination in *Robert Bosch, LLC v. Pylon Manufacturing Corp., 719 F.3d 1305, 1320 (Fed. Cir. 2013)* (en banc) (holding that we retain jurisdiction "to entertain appeals from patent infringement liability determinations when a trial on damages has not yet occurred").

HN2[↑] For patent appeals, we apply the law of the regional circuit, here the Fifth Circuit, to issues not specific to patent law. *LaserDynamics, Inc. v. Quanta Comput., Inc., 694 F.3d 51, 66 (Fed. Cir. 2012)*. The Fifth Circuit reviews motions for summary judgment and motions for judgment as matter of law de novo. *Id.* The Fifth Circuit views all evidence in a light most favorable to the verdict and will reverse a jury's verdict only if the evidence points so overwhelmingly in favor of one party that reasonable jurors could not arrive at any contrary conclusion. *Bagby Elevator Co. v. Schindler Elevator Corp., 609 F.3d 768, 773 (5th Cir. 2010)*. ***HN3***[↑] The ultimate determination **[**7]** of patent eligibility under *35 U.S.C. § 101* is an issue of law we review de novo. *Intellectual Ventures I LLC v. Capital One Fin. Corp., 850 F.3d 1332, 1338 (Fed. Cir. 2017)*. Anticipation and infringement are both questions of fact reviewed for substantial evidence when tried to a jury. *Wi-Lan, Inc. v. Apple Inc., 811 F.3d 455, 461 (Fed. Cir. 2016)*.

[*1440]** I. Patent Eligibility

HN4[↑] Anyone who "invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof" may obtain a patent. *35 U.S.C. § 101*. Because patent protection does not extend to claims that monopolize the "building blocks of human ingenuity," claims directed to laws of nature, natural phenomena, and abstract ideas are not patent eligible. *Alice Corp. Pty. v. CLS Bank Int'l, 134 S. Ct. 2347, 2354, 82 L. Ed. 2d 296, 189 L. Ed. 2d 296 (2014)*. The Supreme Court instructs courts to distinguish between claims that claim patent ineligible subject matter and those that "integrate the building blocks into something more." *Id.* First, we "determine whether the claims at issue are directed to a patent-ineligible concept." *Id. at 2355*. If so, we "examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Id. at 2357* (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 72, 79, 132 S. Ct. 1289, 182 L. Ed. 2d 321 (2012))*. If the claims are directed to a patent-eligible concept, the claims satisfy *§ 101* and we need not proceed to the second step. *Visual Memory LLC v. NVIDIA Corp., 867 F.3d 1253, 1262 (Fed. Cir. 2017)*.

HN5[↑] At step one, **[**8]** we must "articulate what the claims are directed to with enough specificity to ensure the step one inquiry is meaningful." *Thales Visionix Inc. v. United States, 850 F.3d 1343, 1347 (Fed. Cir. 2017)*.

Although there is "difficulty inherent in delineating the contours of an abstract idea," *Visual Memory, 867 F.3d at 1259*, we must be mindful that "all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas." *Mayo, 566 U.S. at 71*. We also ask whether the claims are directed to a specific improvement in the capabilities of computing devices, or, instead, "a process **[*1362]** that qualifies as an 'abstract idea' for which computers are invoked merely as a tool." *Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1336 (Fed. Cir. 2016)*.

We previously have held claims focused on various improvements of systems directed to patent eligible subject matter under *§ 101*. For example, in *Enfish*, we held claims reciting a self-referential table for a computer database eligible under step one because the claims were directed to a particular improvement in the computer's functionality. *822 F.3d at 1336*. That the invention ran on a general-purpose computer did not doom the claims because unlike claims that merely "add[] conventional computer components to well-known business practices," the claimed self-referential table was "a specific type of data structure designed **[**9]** to improve the way a computer stores and retrieves data in memory." *Id. at 1338-39*. In *Thales*, we held claims reciting an improved method of utilizing inertial sensors to determine position and orientation of an object on a moving platform not directed to an abstract idea or law of nature. *850 F.3d at 1349*. We noted that even though the system used conventional sensors and a mathematical equation, the claims specified a particular configuration of the sensors and a particular method of utilizing the raw data that eliminated many of the complications inherent in conventional methods. *Id. at 1348-49*. In *Visual Memory*, we held claims directed to an improved computer memory system with programmable operational characteristics defined by the processor directed to patent-eligible subject matter. *867 F.3d at 1259*. The claimed invention provided flexibility that prior art processors did not possess, and obviated the need to design a separate memory system for each type of processor. *Id.* And most recently, in *Finjan, Inc. v. Blue Coat Systems, Inc.*, we held claims directed to a behavior-based virus scanning method directed to patent eligible subject matter because they "employ[] a new kind of file that enables a computer security system to do things **[**10]** it could not do before," including "accumulat[ing] and utiliz[ing] newly available, behavior-based information about potential threats." *879 F.3d 1299, 2018 U.S. App. LEXIS 601, 2018 WL 341882 (Fed. Cir. Jan. 10, 2018)*. The claimed behavior-based scans, in contrast to prior art systems which searched for matching code, enabled more "nuanced virus filtering" in analyzing whether "a downloadable's code . . . performs potentially dangerous or unwanted operations." *2018 U.S. App. LEXIS 601, [WL] at *3*. We held the claims "therefore directed to a non-abstract improvement in functionality, rather than the abstract idea of computer security writ large." *2018 U.S. App. LEXIS 601, [WL] at *4*.

The asserted claims in this case are directed to an improved user interface for computing **[***1441]** devices, not to the abstract idea of an index, as argued by LG on appeal.[3] Although the generic idea of summarizing information certainly existed prior to the invention, these claims are directed to a particular manner of summarizing and presenting information in electronic devices. Claim 1 of the '476 patent requires "an application summary that can be reached directly from the menu," specifying a particular manner by which the summary window must be accessed. The claim further requires the application summary window list a limited set of data, "each of the data in the list being **[**11]** selectable to launch the respective application and enable the selected data to be seen within the respective application." This claim limitation **[*1363]** restrains the type of data that can be displayed in the summary window. Finally, the claim recites that the summary window "is displayed while the one or more applications are in an unlaunched state," a requirement that the device applications exist in a particular state. These limitations disclose a specific manner of displaying a limited set of information to the user, rather than using conventional user interface methods to display a generic index on a computer. Like the improved systems claimed in *Enfish*, *Thales*, *Visual Memory*, and *Finjan*, these claims recite a specific improvement over prior systems, resulting in an improved user interface for electronic devices.

The specification confirms that these claims disclose an improved user interface for electronic devices, particularly those with small screens. It teaches that the prior art interfaces had many deficits relating to the efficient functioning of the computer, requiring a user "to scroll around and switch views many times to find the right data/functionality." '020 patent at 1:47-49. Because **[**12]** small screens "tend to need data and functionality divided into many layers or views," *id.* at

[3] This articulation of the purported abstract idea was advanced for the first time on appeal. Because we do not find this theory or the theory offered below to be well-taken, we do not decide whether the argument was waived, as Core Wireless argues.

1:29-30, prior art interfaces required users to drill down through many layers to get to desired data or functionality. *Id.* at 1:29-37. That process could "seem slow, complex and difficult to learn, particularly to novice users." *Id.* at 1:45-46.

The disclosed invention improves the efficiency of using the electronic device by bringing together "a limited list of common functions and commonly accessed stored data," which can be accessed directly from the main menu. *Id.* at 2:55-59. Displaying selected data or functions of interest in the summary window allows the user to see the most relevant data or functions "without actually opening the application up." *Id.* at 3:53-55. The speed of a user's navigation through various views and windows can be improved because it "saves the user from navigating to the required application, opening it up, and then navigating within that application to enable the data of interest to be seen or a function of interest to be activated." *Id.* at 2:35-39. Rather than paging through multiple screens of options, "only three steps may be needed from start up to reaching **[**13]** the required data/functionality." *Id.* at 3:2-3. This language clearly indicates that the claims are directed to an improvement in the functioning of computers, particularly those with small screens.

Because we hold that the asserted claims are not directed to an abstract idea, we do not proceed to the second step of the inquiry. The claims are patent eligible under *§ 101*.

II. Anticipation

The Blanchard reference teaches a display screen for mobile phones that "provides an arrangement for dynamically varying how space on a small display is allocated for presentation of various types of user information." J.A. 13097 at 1:53-57. It discloses hierarchical menu screens displaying a series of selectable sub-level menu choices through which a user can cycle. The display changes dynamically as the user makes selections; for example, selecting a function, such as "phone book," will display options related to that function, such as "add entry."

LG argues it established by clear and convincing evidence that Blanchard discloses each element of the asserted claims. It first submits that Core Wireless based its arguments distinguishing the asserted claims from Blanchard during closing argument and post-trial **[**14]** briefing on elements not recited by the asserted claims. It further submits that, because it presented a prima facie case of anticipation and Core Wireless failed to present any affirmative **[*1364]** evidence in rebuttal, it is entitled to judgment as a matter of law that Blanchard anticipates the asserted claims. We disagree.

[*1442]** HN6[] A patent is presumed valid, and the burden of establishing invalidity of a claim rests on the party asserting invalidity by clear and convincing evidence. 35 U.S.C. § 282; Microsoft Corp. v. i4i Ltd. P'ship, 564 U.S. 91, 95, 131 S. Ct. 2238, 180 L. Ed. 2d 131 (2011). An alleged infringer asserting a defense of invalidity also has "the initial burden of going forward with evidence to support its invalidity allegation." Titan Tire Corp. v. Case New Holland, Inc., 566 F.3d 1372, 1376 (Fed. Cir. 2009). Once that evidence has been presented, the "burden of going forward shifts to the patentee to present contrary evidence and argument." Id. at 1376-77. Ultimately, however, the outcome of an alleged infringer's invalidity defense at trial depends on whether the alleged infringer "has carried its burden of persuasion to prove by clear and convincing evidence that the patent is invalid." Id. at 1377. Because the burden rests with the alleged infringer to present clear and convincing evidence supporting a finding of invalidity, granting judgment as a matter of law for **[**15]** the party carrying the burden of proof is generally "reserved for extreme cases," such as when the opposing party's witness makes a key admission. 9B Fed. Prac. & Proc. Civ. § 2535 (3d ed.); *see* Grey v. First Nat'l Bank in Dall., 393 F.2d 371, 380 (5th Cir. 1968) ("[W]hen the party moving for a directed verdict has such a burden, the evidence to support the granting of the motion must be so one-sided as to be of overwhelming effect.").

This is not one such extreme case. While LG presented the testimony of Dr. Rhyne, the only expert who testified regarding anticipation, Core Wireless cross-examined Dr. Rhyne, illuminating for the jury reasons why Dr. Rhyne's opinion was incorrect. For example, Dr. Rhyne testified that Blanchard discloses the "limited list" of data and functions recited in the asserted claims because Blanchard Figure 3 displays only three of the five functions of the phone book application. But on crossexamination, when asked if all five functions were "available through this menu," Dr. Rhyne admitted that all five functions of the phone book application were available through Blanchard's disclosed menus: "You can reach all of them—you can bring them all to the face of the screen, if that's what you mean." J.A. 10741. Viewing the evidence **[**16]** in the light most favorable to the verdict, we cannot say that this is a case in which the evidence points so strongly and overwhelming in

favor of LG that reasonable jurors could not arrive at any contrary conclusion. A reasonable jury could have heard the cross-examination of Dr. Rhyne and concluded Blanchard did not disclose the "limited list" limitation in the claims because a user could access the additional functions in Blanchard by keying down within the summary display window. Core Wireless had the right to choose to use its limited trial clock for other purposes where it believed—perhaps at its own risk—that LG's evidence had been adequately impeached. And the jury was entitled to evaluate Dr. Rhyne's testimony and determine whether LG clearly and convincingly established that Blanchard anticipates the claims.

The district court, in denying LG's motion for judgment as a matter of law, did not hold that the presumption of validity "saved" the claims in the face of unrebutted evidence. The court merely made the unremarkable observation that the jury was not required "to give full credit and acceptance to the testimony of Dr. Rhyne." J.A. 17. We agree with the district court and **[**17]** affirm its denial of LG's motion for judgment as a matter of law of anticipation.

[*1365] III. Infringement

LG presents two noninfringement arguments on appeal. First, LG argues the correct construction of "unlaunched state" is "not running," rather than "not displayed" as the district court held, and the accused devices do not infringe under its proposed construction.[4] Second, LG argues that no reasonable jury could find that the accused devices satisfy the "reached directly from the [main] menu" limitations in the claims because the accused application summary window is reached from the status bar, which is not part of the menu. We reject both arguments.

HN7[] "[T]he ultimate issue of the proper construction of a claim should be treated as a question of law," which we review de novo. *Teva Pharms. USA, Inc. v. Sandoz, Inc., 135 S. Ct. 831, 838, 190 L. Ed. 2d 719 (2015)*. Any subsidiary factual findings **[***1443]** related to claim construction are reviewed under the clearly erroneous standard. *Id.* In construing the claims, we consider "the words of the claims themselves, the specification, the prosecution history, and if necessary, any relevant extrinsic evidence." *Advanced Steel Recovery, LLC v. X-Body Equip., Inc., 808 F.3d 1313, 1317 (Fed. Cir. 2015)*. "[W]hen the district court reviews only evidence intrinsic to the patent (the patent claims and specifications, along with the patent's **[**18]** prosecution history), the judge's determination will amount solely to a determination of law." *Teva Pharms. USA, Inc., 135 S. Ct. at 841*.

First, we consider the construction of "unlaunched state." While this is a close case for which the intrinsic evidence could plausibly be read to support either party, we see no error in the district court's construction of "unlaunched state" to mean "not displayed." Such a construction encompasses both applications that are not running at all and applications that are running, at least to some extent, in the background of the electronic device. *See* J.A. 10283 (Core Wireless' expert testifying that an unlaunched application is "either not executing code or not visible to the user").

The stated focus of the invention is to "allow the user to navigate quickly and efficiently to access data and activate a desired function" on devices with small screens. '020 patent at 1:26-29. The invention identifies as problematic the conventional user interfaces in which "a user may need to scroll around and switch views many times to find the right data/functionality." *Id.* at 1:47-49. For instance, the specification does not identify the memory drain that running applications may have on the system as a problem it **[**19]** aims to solve—it only concerns itself with maximizing the benefit of the "common functions and commonly accessed data" actually displayed to the user. *Id.* at 2:26-30; *see id.* at 4:36-39 ("The mobile telephone may be able to learn what functionality and/or stored data types are most likely to be of interest to a given user and which should therefore be included in a summary view to any given user.").

The terms "display" and "launch" are used throughout the specification to convey that a particular view is displayed to the user. The specification states the following when describing the advantages in user navigation achieved by the invention:

> [A] user can get to the summary window in just two steps—first, *launch a main view* which shows various applications; then, *launch the appropriate summary window* for the application of interest. This is far faster and easier than conventional **[*1366]** navigation approaches. Once *the*

[4] On appeal, LG does not dispute that under the court's construction of "unlaunched state," substantial evidence supports the jury's verdict that the accused devices meet this limitation.

> *summary window is launched, core data/functionality is displayed* and can be accessed in more detail can typically be reached simply by selecting that data/functionality.

Id. at 2:59-3:2 (emphases added). In this passage, "launch" is used to describe what is displayed to the user **[**20]** when they select various menu options, not to indicate that an application is running.

This understanding is confirmed by the patents' use of the word "running." While the specification uses the term "display" throughout, it only uses the term "running" (or any modification of the term) one time: "there is a computer program which when running on a computing device (such as a mobile telephone), enables the device to operate in accordance with the above aspects of the invention. The program may be an operating system." *Id.* at 2:40-44. Therefore, when the patent teaches that a user "launch[es] a main view" or "launch[es] the appropriate summary window," the computer program or operating system implementing the summary program is already running. *Id.* at 2:59-3:2. Similarly, each patent only has one independent claim which uses the term "running," and it is used to describe the overall "computer program product" that implements the claimed functionality, not a device application. '020 patent at 6:20-32 (claim 16); '476 patent at 6:30-43 (claim 11). These claims further recite an application "in an unlaunched state." If the patentee intended "unlaunched" to mean "not running," it knew how to express as much.

[21]** Figure 3, which is identical for both patents, further confirms this construction of "unlaunched state." In Figure 3, the summary window indicates that under the "Messages" application there are "3 unread emails," "2 new SMS" messages, and "1 Chat *ongoing."* '020 patent at Fig. 3 (emphasis added). The use of the word "ongoing" (as opposed to a word like "received") indicates that, in at least some embodiments of the invention, at least some subset of processes of **[***1444]** the Messages application are already running. The specification confirms that the application summary window reflects information that is something more than mere notifications from an application: "App Snapshots are not intended to replace notifications, but to complement them by providing non-intrusive reminders for the user, as well as rapid shortcuts to key application functionality." *Id.* at 4:32-35.

The specification also describes a preferred embodiment in which "the constituency of the App Snapshot may *vary with the environment* in which the mobile telephone finds itself." *Id.* at 4:47-49 (emphasis added). It explains "if the telephone is Bluetooth enabled, then there may be a Bluetooth application which has associated with it a summary window which lists the other Bluetooth devices in the vicinity." *Id.* at 4:49-52. Moreover, claim 6 of the '020 patent and claim 5 of the '476 patent both require that the data or functionality displayed "varies with the environment of the device." LG has not articulated how an application with data in the application summary window that *varies* as the location of the device changes can operate without having the application "running" in some manner. While the full Bluetooth application may not be "running," at least some subset of that application's processes must be running in order to update the available **[**22]** devices in the application summary window.

The Bluetooth embodiment and the Messages embodiment displayed in Figure 3 are consistent with Core Wireless' argument during the *O2 Micro* hearing that a launched application is executing code *and* visible to the user. An unlaunched application, therefore, is "*either* not executing **[*1367]** code *or* not visible to the user." J.A. 10283 (emphases added). The specification does not teach that the application summary window performs limited processes on behalf of the unlaunched applications. LG's proposed construction of "unlaunched" as "not running" would impermissibly read these preferred embodiments out of the claims.

LG argues that the specification uses "launch" and "display" to express different ideas. For example, the specification explains: "The App Snapshot can therefore *display* data from an application and functions of that application *without actually opening the application up:* only once a user has selected an item in the App Snapshot associated with a given application does that application have to be opened." '020 patent at 3:53-58 (emphases added). This passage does not contradict the district court's construction. The passage does not state that the **[**23]** application summary window displays the *application* without actually opening the application up. The specification's statement that the App Snapshot "display[s]" *data* without the selected application being "opened" does not, without more, indicate that a previously unopened application was not running at least some subset of processes. Similarly, the dissent's interpretation assumes that displaying an application necessarily requires display of particular data. Wallach Op. at 3-5. The specification demonstrates this not to be true. When a user selects

data from the summary window, e.g., a commonly emailed contact, "the display then changes to a new email form seeded with [the] email address and all the user need do is input some body text and hit a 'Do It' button." '020 patent at 5:5-19. This is different from displaying an email application without this preloaded data, which does not "enable the selected data to be seen within the respective application." '476 patent claim 1.

The patentee did not clearly and unmistakably disclaim or limit the construction of "unlaunched state" during prosecution, as LG argues. ***HN8***[↑] The doctrine of prosecution disclaimer precludes patentees from recapturing the full scope of **[**24]** a claim term only when the patentee clearly and unmistakably disavows a certain meaning in order to obtain the patent. *Mass. Inst. of Tech. v. Shire Pharms., Inc., 839 F.3d 1111, 1119 (Fed. Cir. 2016)*. When the alleged disclaimer is ambiguous or amenable to multiple reasonable interpretations, we decline to find prosecution disclaimer. *Id.*

The patentee's statements during prosecution do not amount to a clear and unmistakable disclaimer restricting the meaning of "unlaunched state" only to those applications that are not running any processes. During prosecution, the patentee distinguished the claims from prior art U.S. Patent No. 6,781,611 ("Richard"). Richard teaches a method "for switching between multiple open windows in multiple applications on a computer desktop." J.A. 14461 at 1:38-40. The examiner pointed to Richard Figure 6, in which "the user has two applications, AppA and AppB . . . open on a desktop," the top **[***1445]** window being AppA. J.A. 14459, 14462 at 3:20-26. A plurality of windows are open within AppB, and when the user clicks and holds the arrow on the application button for AppB on the taskbar, a popup menu appears, displaying the three open windows within AppB. In distinguishing the invention from Richard, the patentee stated that the main menu of Richard is "a menu of *open* ***[**25]*** windows within a single application, i.e., a launched application. It follows from the fact the windows are open within the application that the application must be running and therefore has been launched." J.A. 12764 (emphases in original). This statement is consistent with the district court's construction. Both AppA and AppB in Richard Figure 6 are **[*1368]** displayed to the user. While AppA takes up most of the display area in this figure, AppB is also displayed to the user in the form of the application button on the taskbar. Indeed, Richard specifically teaches that the arrow on the application button for AppB "serves as a *visual indicator* that there are a plurality of windows open in AppB." J.A. 14462 at 3:35-37 (emphasis added). Core Wireless admits that an application that is displayed must be running. Oral Arg. at 20:32-40. Because AppB in Richard Figure 6 is displayed and running, the patentee's statement during prosecution that AppB must be "launched" is fully consistent with the construction that "unlaunched state" means "not displayed."

Because the claim language, specification, and prosecution history all support the district court's construction, we agree with the district court **[**26]** that the correct construction of "unlaunched state" is "not displayed."

Second, substantial evidence supports the jury's verdict of infringement based on the "reached directly from the [main] menu" claim limitation. LG argues no reasonable jury could find the accused devices satisfy this limitation because the evidence at trial established that the status bar was distinct from a "main menu." We do not agree.

There is no dispute on appeal how the accused devices work. The devices have a primary home screen display, comprising a series of icons along the bottom of the display, corresponding to applications like Gmail and Phone. The entire home screen display is the accused "main menu." Along the top of the home screen display, a status bar displays the time, battery status, signal strength, and other data. The accused application summary window is the LG devices' notification shade, which the user accesses by swiping down from the status bar.

The jury heard conflicting evidence regarding whether the status bar is part of the accused "home screen." Dr. Rhyne testified that the status bar is "not part of the home screen" because the home screen is the part of the screen between the status **[**27]** bar at the top and the navigation bar at the bottom of the display. J.A. 10603-04. He further testified that the user "can open [the notification shade] up in almost any application," not just the main home screen view. J.A. 10604-05. Core Wireless' infringement expert agreed that a user can reach the notification shade from the status bar while any application is displayed in the central view. Core Wireless presented evidence, however, that the status bar is part of the home screen. Core Wireless' expert, Dr. Zeger, acknowledged that when an application is open and displayed, the user does not reach the notification shade directly from the main menu "because there was an intervening step" of opening up the

application from the main menu. J.A. 10315. But he testified that when the main menu is displayed and the user pulls down the notification shade, the user reaches the accused application summary window directly from the main menu. Core Wireless also presented LG's user manual to the jury, which expressly identifies the status bar as part of the home screen.

The parties' dispute boils down to whether the status bar is part of the accused "home screen." This is a fact question that **[**28]** we presume the jury resolved in favor of Core Wireless, and substantial evidence supports the jury's finding. In the LG user manual, the status bar is the first section of the view identified as the home screen. The jury was also entitled to credit Dr. Zeger's testimony on this issue. Indeed, Dr. Rhyne admitted that if the status bar is part of the home screen, the user can reach the accused application summary window directly from the main **[*1369]** menu. We conclude that substantial evidence supports the jury's finding of infringement.

CONCLUSION

For the foregoing reasons, we affirm the district court's denial of summary judgment that the claims are ineligible under *35 U.S.C. § 101*. We also affirm the district court's denial of judgment as a matter of law that the **[***1446]** claims are anticipated by Blanchard and the claims are not infringed.

AFFIRMED

Concur by: WALLACH (In Part)

Dissent by: WALLACH (In Part)

Dissent

WALLACH, *Circuit Judge*, concurring-in-part and dissenting-in-part.

I agree with the majority that the U.S. District Court for the Eastern District of Texas ("District Court") did not err either in determining that claims 11 and 13 of U.S. Patent No. 8,434,020 ("the '020 patent") and claims 8-9 of U.S. Patent No. 8,713,476 ("the '476 patent") (collectively, the "Asserted Claims") (together, the "Patents-in-Suit") are patent eligible **[**29]** or in construing the "reached directly" claim limitation for purposes of its infringement and anticipation analyses. *See* Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc., No. 2:14-cv-911-JRG, 2016 U.S. Dist. LEXIS 112425, 2016 WL 4440255, at *1 (E.D. Tex. Aug. 23, 2016) (ruling on anticipation and infringement); Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc., No. 2:14-cv-911-JRG-RSP, 2016 U.S. Dist. LEXIS 35663 (Tex. Mar. 20, 2016) (J.A. 9555-62) (ruling on eligibility). I disagree, however, with the majority's ruling affirming the District Court's construction of the "unlaunched state" limitation. *See* '476 patent col. 6 ll. 2-3; '020 patent col. 5 l. 43. I would find the term "unlaunched state" to mean "not running," as proposed by Appellant LG Electronics, Inc. ("LG"), and remand the case to the District Court for review of whether this construction alters its findings on infringement and anticipation.[1] I therefore respectfully dissent-in-part from today's judgment. I review the legal standard for claim construction and then turn to my analysis.

I. Legal Standard

Claim construction focuses on the wording of the claims, "read in view of the specification, of which they are a part." Phillips v. AWH Corp., 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (internal quotation marks and citation omitted). Prosecution history may also be examined to supply additional **[**30]** context to support a claim term's intended meaning. *See* Home Diagnostics, Inc. v. Lifescan, Inc., 381 F.3d 1352, 1356 (Fed. Cir. 2004). While courts may consider extrinsic evidence in claim construction, "such evidence is generally of less significance than the intrinsic record." Wi-LAN, Inc. v. Apple Inc., 811 F.3d 455, 462 (Fed. Cir. 2016) (citation omitted). Extrinsic evidence may not be used "to contradict claim meaning that is unambiguous in light of the intrinsic evidence." Phillips, 415 F.3d at 1324 (citation omitted). The District Court did not analyze extrinsic evidence in making its determination. *See* J.A. 10277-97. When the district court reviews only evidence intrinsic to the patent, that determination will amount solely to a determination of law that we review de novo. *See* Teva Pharms. USA, Inc. v. Sandoz, Inc., 135 S. Ct. 831, 841, 190 L. Ed. 2d 719 (2015).

II. The District Court Erred in Its Claim Construction of "UnLaunched State"

The District Court construed the term "unlaunched state" during a pretrial conference **[*1370]** to mean "not

[1] Neither party argued that a different claim construction would affect our analysis of eligibility. *See generally* Appellant's Br.; Appellee's Br.

displayed" and maintained that construction in its post-trial denial of judgment as a matter of law. *See* Core Wireless, 2016 U.S. Dist. LEXIS 112425, 2016 WL 4440255, at *4-5; J.A. 10297. LG argues that the term "unlaunched state" should mean "not running." Appellant's Br. 30; *see id*. at 30-48. I agree with LG. Consistent with claim construction principles, I look first to the language of the claims, followed by the remainder of the specification's language and prosecution **[**31]** history. *See* Phillips, 415 F.3d at 1315.

First, the claims state in part that: an application summary "displays" certain data offered in applications; each of the data is "selectable to launch the respective application and enable the selected data to be seen"; *and* the application summary is "displayed while the one or more applications are in an unlaunched state." '476 patent col. 5 l. 60-col. 6 l. 3 (claim 1).[2] "Display" is used differently and independently from "launch" in the claims, which indicates these terms have different meanings. In addition, by separating "launch" and "enable the selected data to be seen," the claims contemplate a difference between launching and displaying data. *See* Chi. Bd. Options Exch., Inc. v. Int'l Sec. Exch., ***[***1447]*** LLC, 677 F.3d 1361, 1369 (Fed. Cir. 2012) (applying a "general presumption that different [claim] terms have different meanings"). Further, the claim language distinguishes between "launch[ing] the respective application" itself, and "enab[ling] the selected data . . . *within"* the application to be seen. '476 patent col. 5 l. 66-col. 6 l. 1 (emphasis added). Such a distinction would be rendered meaningless if launch were construed to mean "display." *See* Merck & Co. v. Teva Pharms. USA, Inc., 395 F.3d 1364, 1372 (Fed. Cir. 2005) ("A claim construction that gives meaning to all the terms of the claim is preferred over one that does not do so." (citation **[**32]** omitted)). Moreover, I do not understand what "displaying" the application itself would mean in this context, where the claim language more specifically directs the invention to enable only certain "data" previewed in the application summary to be seen. *See* Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc., 381 F.3d 1111, 1119 (Fed. Cir. 2004) ("[W]hen an applicant uses different terms in a claim it is permissible to infer that he intended his choice of different terms to reflect a differentiation in meaning of those terms.").

Second, the specification uses the terms "launch" and "display" distinctly. *See* '476 patent col. 3 ll. 10-11 ("Once the summary window is launched, core data/functionality is displayed."). This could either mean the terms are distinct, or, as the majority finds, that launch is synonymous with display. *See* Maj. Op. at 14-17. As stated previously, based on claim differentiation principles, I find it more likely that "launch" is a first step of independent meaning, and "display" is a step that comes second, after the "summary window" has been launched. Appellee Core Wireless Licensing S.A.R.L. ("Core Wireless") contends that the statement "a user can . . . launch a main view which shows various applications," '476 patent col. 3 ll. 5-7, supports its argument that "launch" **[**33]** refers to granting "visual access," because the language of the specification uses the term "view," Appellee's Br. 21. However, the term "main view" refers to and is synonymous with the summary application window. *See* '476 patent col. 3 ll. 5-7, 17-33; *id.* figs.1-3. Referring to this particular page using the term "view" does not confer additional meaning on the verb "launch."

[*1371] Additional language in the specification in support of LG's construction states that previously, users would "locate," "then start/open the required application," "*and then* may need to . . . cause the required stored data . . . to be displayed." *Id.* col. 1 ll. 51-55 (emphasis added). Again, the specification contemplates display and opening as two separate steps in the user's process, which leads me to the conclusion that "display" and "open" are not synonymous, and that the drafters of the Patents-in-Suit knew how to use the term "display" when conveying visual access to an application's contents.[3]

I also note that the specification explicitly defines the term "idle screen" as "a display which is shown when the mobile telephone is switched on but not in use," *id.* col. 2 ll. 10-12, which indicates the drafters of the Patents-in-Suit **[**34]** knew how to define a single term that contained two separate meanings (here, one related to display, and one related to operation), and believed such an explanation would be necessary for terms that on their face did not contain a dual meaning. For that reason, I am skeptical of the majority's understanding that the term "unlaunched"

[2] Claim 1 of the '020 patent is substantively similar to the relevant portions of the '476 patent and the specifications are effectively identical, so I refer only to claim 1 of the '476 patent for ease of reference.

[3] For the same reason, I do not agree with the majority's conclusion that certain passages in the specification use "launch" to describe "what is displayed to the user when they select various menu options." Maj. Op. at 15 (citing '020 patent col. 2 l. 59-col. 3 l. 2).

"encompasses both applications that are not running at all and applications that are running, at least to some extent, in the background of the electronic device."[4] Maj. Op. at 14.

I also agree with LG's contention that the specification teaches the invention was directed to a problem in line with its construction of the term "unlaunched state," or, at least, that the problems in the field are inconclusive to weigh in favor of either party's proposed construction. LG asserts that the invention is directed to saving "the user from navigating **[***1448]** to the required application, opening it up, and then navigating within that application." Appellant's Br. 32 (quoting '476 patent col. 2 ll. 46-50). Again, construction hinges on our understanding of the term "open" in this phrase and whether it refers to running or displaying an application. No matter the construction of launch **[**35]** though, the claimed invention seeks to improve access to the large amount of information stored in small computing devices. *See, e.g.*, '476 patent col. 2 l. 66-col. 3 l. 6 (discussing invention's "advantages in ease and speed of navigation, particularly on small screen devices"). It seems to me that the default state of the applications storing this information when a user navigates through the claimed summary application menu does not affect the utility of the claimed invention.

The majority identifies the stated focus of the inventions as to "allow the user to navigate quickly and efficiently to access data and activate a desired function" on small screens. Maj. Op. at 14 (quoting '020 patent col. 1 ll. 26-29). Therefore, it finds the absence of an explicitly stated goal such as "memory drain," a problem which appears to be of the majority's own creation, to be instructive in its construction of the term "unlaunched," because the invention "only concerns itself with maximizing the benefit of the 'common functions and commonly accessed data' actually **[*1372]** displayed to the user." *Id.* at 15 (quoting '020 patent col. 4 ll. 36-39). In our claim construction analysis, we look not to what is absent from the specification or what could **[**36]** have been written, but rather to what is included. *See* Merck & Co. v. Teva Pharms. USA, Inc., 347 F.3d 1367, 1371 (Fed. Cir. 2003) ("A fundamental rule of claim construction is that the terms in a patent document are construed with the meaning with which they are presented *in the patent document*. Thus claims must be construed so as to be consistent with the specification . . . ." (emphasis added) (citations omitted)). Here, as mentioned above, the focus of the invention identified by the majority can support either party's construction of the disputed term. The use of an application summary menu to congregate data from myriad applications on a small screen computing device benefits users in the manner stated, regardless of whether the applications are running in the background. Moreover, in other parts of the specification, the invention is directed towards "effectively enabling the user to understand th[e device's] changing internal state" through offering on the application menu page a list of "common functions offered within an application and/or . . . data stored in that application." '476 patent col. 2 ll. 22-24, 34-36. Here again, enabling a user to better understand options offered by applications and data *stored* within them are goals that are successfully achieved **[**37]** with applications that are not running until selected from the main menu.

Third, the prosecution history further supports LG's proffered construction. Even if Core Wireless did not disclaim its professed interpretation that "launch" means "display,"[5] I would nevertheless find LG's interpretation of "unlaunched" comports more closely with the overall language of the Patents-in-Suit and prosecution history. *See* Phillips, 415 F.3d at 1316. Indeed, during prosecution, Core Wireless distinguished the Asserted Claims from those in the prior art because, unlike the prior art, its claims did not "only ever display[]" the summary application menu "within a running instance of the program, i.e., only when the program is in a *launched* state." J.A. 12764 (emphasis added). Thus, Core Wireless used the term "launch" to mean running, not merely displayed. *See* J.A. 12765 (stating, in another portion of Core Wireless's amendment, that 1) the "underlying purpose" of the claimed invention is that it overcomes the prior art in which information about applications in the summary application menu "is not

---

[4] While the majority additionally supports its argument by referring to the single use of the term "running" in the specification, *see* Maj. Op. at 15-16 (quoting '020 patent col. 2 ll. 40-44 ("[T]here is a computer program which when running on a computing device . . . ."), I note that neither party made arguments with respect to this language, and it is not clear to me from the record that "running" when referring to the computer program itself equates to use of the term as applied to applications within the device.

[5] Both the majority and the District Court interpret LG's arguments as prosecution disclaimer arguments and determine that LG does not meet the high bar to prove that Core Wireless "clearly disavowed claim scope during prosecution." Core Wireless, 2016 U.S. Dist. LEXIS 112425, 2016 WL 4440255, at *4; *see* Maj. Op. at 18-19.

displayed until after the application is already running" and 2) the prior art "*relate*[*s] to running applications* and combining **[**38]** them does nothing to satisfy the requirement of the present claims that the application summary window is displayed without launching the application" (emphasis added)).

The majority adopts Core Wireless's argument that construing "unlaunched" to mean "not running" would exclude certain preferred embodiments in the specification, *see* Maj. Op. at 16-17; *see also* Appellee's Br. 28-29, contrary to our court's instruction that a **[***1449]** construction "that excludes a preferred embodiment from the scope of the claim is rarely, if ever, correct," *MBO Labs., Inc. v. Becton, Dickinson & Co., 474 F.3d 1323, 1333 (Fed. Cir. 2007)* (internal quotation marks and citation omitted). Specifically, Figure 3 illustrates an application window that indicates there is an ongoing chat not seen on the **[*1373]** screen. *See* '020 patent fig.3; '476 patent fig.3. The majority states that "use of the word 'ongoing' (as opposed to a word like 'received') indicates that, in at least some embodiments of the invention, at least some subset of processes of the Messages application are already running." Maj. Op. at 16. Yet Core Wireless has not presented evidence, in the form of expert testimony or otherwise, to suggest that the display in the application menu of new messages or the use of the term ongoing in the summary menu would **[**39]** be understood by a person having ordinary skill in the art to indicate the underlying application is running. Core Wireless presents only attorney argument, not evidence. *See Gemtron Corp. v. Saint-Gobain Corp., 572 F.3d 1371, 1380 (Fed. Cir. 2009)* ("[U]nsworn attorney argument . . . is not evidence and cannot re-but . . . admitted evidence." (citation omitted)); Appellee's Br. 28-29. Moreover, I do not believe construing "unlaunched" to mean "not running" would be inconsistent with this preferred embodiment, since the requirements of claim 1 only state that "one or more applications" are in an unlaunched state. '476 patent col. 6 ll. 2-3; *see* '020 patent col. 5 ll. 35, 43 (requiring "at least a first application" that is "in an unlaunched state"). Therefore, even if "ongoing" were to imply a running application, the application menu display of messages from a non-running message application would still satisfy the requirements of claim 1 of the Patents-in-Suit.[6]

Accordingly, I would reverse the District Court's claim construction of "un-launched state" and construe the term to mean "not running." Given this claim construction, I would remand for further findings on infringement and anticipation. I respectfully dissent.

End of Document

[6] I would not read lines in the specification stating that "App Snapshots are not intended to replace notifications, but to complement them by providing non-intrusive reminders for the user" to support "launch" meaning "display," as the majority contends. See Maj. Op. at 16; '476 patent col. 4 ll. 43−46; '020 patent col. 4 ll. 32−35. Such language could just as easily be understood to refer to a summary application menu's presentation of information from applications that are not currently running.

Data Engine Techs. LLC v. Google LLC

United States Court of Appeals for the Federal Circuit

October 9, 2018, Decided

2017-1135

Reporter
906 F.3d 999 *; 2018 U.S. App. LEXIS 28412 **; 2018 WL 4868029

DATA ENGINE TECHNOLOGIES LLC, Plaintiff-Appellant v. GOOGLE LLC, Defendant-Appellee

Prior History: [1]** Appeal from the United States District Court for the District of Delaware in No. 1:14-cv-01115-LPS, Chief Judge Leonard P. Stark.

Data Engine Techs. LLC v. Google Inc., 211 F. Supp. 3d 669, 2016 U.S. Dist. LEXIS 134002 (D. Del., Sept. 29, 2016)

Disposition: AFFIRMED-IN-PART, REVERSED-IN-PART, AND REMANDED.

Core Terms

spreadsheet, patent, tabs, user, electronic, recite, display, cell, three-dimensional, interface, invention, abstract idea, navigating, notebook, identifier, district court, pages, asserted claim, changes, storing, improved, functionality, eligibility, patent-ineligible, comprising, commands, tracking, prior art, ineligible, organizing

Case Summary

Overview
HOLDINGS: [1]-The district court erred, with one exception, when it found that claims in U.S. Patent Nos. 5,590,259, 5,784,545, and 6,282,551 ("the '551 patent") which claimed systems and methods for making complex electronic spreadsheets more accessible by providing notebook tabs could not be patented under *35 U.S.C.S. § 101* because they were directed to abstract ideas and failed to provide an inventive concept; [2]-The evidence supported the district court's judgment that claim 1 in the '551 patent was not patentable under *§ 101* because it was directed to the abstract idea of identifying and storing electronic spreadsheet pages; [3]-The district court did not err when it found that claims in U.S. Patent No. 5,303,146 which recited methods for tracking changes to data in spreadsheets were not patentable under *§ 101* because they were directed to an abstract idea.

Outcome
The court affirmed the district court's judgment in part, reversed it in part, and remanded the case.

LexisNexis® Headnotes

Civil Procedure > Appeals > Standards of Review > De Novo Review

Patent Law > Jurisdiction & Review > Standards of Review > De Novo Review

Civil Procedure > Judgments > Pretrial Judgments > Judgment on Pleadings

Patent Law > Subject Matter

HN1 **Standards of Review, De Novo Review**

The United States Court of Appeals for the Federal Circuit reviews a district court's judgment on the pleadings under regional circuit law. The United States Court of Appeals for the Third Circuit reviews the grant of judgment on the pleadings de novo, accepting all of the allegations in the pleadings of the party against whom the motion is addressed as true and drawing all reasonable inferences in favor of the nonmoving party. Patent eligibility can be determined on the pleadings under *Fed. R. Civ. P. 12(c)* when there are no factual allegations that, when taken as true, prevent resolving the eligibility question as a matter of law.

Patent Law > Jurisdiction & Review > Standards of Review

Patent Law > Subject Matter

HN2 **Jurisdiction & Review, Standards of Review**

35 U.S.C.S. § 101 provides that whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor. In Alice Corp. v. CLS Bank International, the United States Supreme Court articulated a two-step test for examining patent eligibility under *§ 101*. Under that test, the United States Court of Appeals for the Federal Circuit must first determine whether the claims at issue are directed to a patent-ineligible concept. Laws of nature, natural phenomena, and abstract ideas are not patentable. The "abstract ideas" category embodies the long-standing rule that an idea of itself is not patentable. If a patent's claims are not directed to a patent-ineligible concept under Alice step 1, they satisfy *§ 101* and the Federal Circuit need not proceed to the second step. If the claims are directed to a patent-ineligible concept, however, the Federal Circuit considers Alice step two.

Patent Law > Jurisdiction & Review > Standards of Review

Patent Law > Subject Matter

HN3 **Jurisdiction & Review, Standards of Review**

In the second step of the two-step test the United States Supreme Court adopted in Alice Corp. v. CLS Bank International for examining patent eligibility under *35 U.S.C.S. § 101*, the United States Court of Appeals for the Federal Circuit considers the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application. The second step is a search for an inventive concept—i.e., an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.

Civil Procedure > Judgments > Pretrial Judgments > Judgment on Pleadings

Patent Law > Infringement Actions > Prosecution History Estoppel > Prosecution Related Arguments & Remarks

HN4 **Pretrial Judgments, Judgment on Pleadings**

On a motion for judgment on the pleadings, a court may consider matters of public record. Prosecution histories constitute public records in patent infringement actions.

Patent Law > Jurisdiction & Review > Standards of Review

Patent Law > Subject Matter

HN5 **Jurisdiction & Review, Standards of Review**

At Alice step one, it is not enough to merely identify a patent-ineligible concept underlying a claim; instead, the United States Court of Appeals for the Federal Circuit must determine whether that patent-ineligible concept is what the claim is "directed to." And that inquiry requires that the claims be read as a whole.

Patent Law > Claims & Specifications > Claims > Claim Language

Patent Law > Subject Matter

Patent Law > Jurisdiction & Review > Standards of Review

HN6 **Claims, Claim Language**

The question of abstraction is whether a patent's claim is "directed to" the abstract idea itself, and the United States Court of Appeals for the Federal Circuit must consider the claim as a whole to determine whether the claim is directed to an abstract idea or something more.

Patent Law > ... > Utility Patents > Process Patents > Computer Software & Mental Steps

Patent Law > Subject Matter

HN7 **Process Patents, Computer Software &**

Mental Steps

The mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention. For the role of a computer in a computer-implemented invention to be deemed meaningful in the context of the Alice/Mayo analysis, it must involve more than performance of well-understood, routine, and conventional activities previously known to the industry.

Counsel: BENJAMIN F. FOSTER, Ahmad, Zavitsanos, Anaipakos, Alavi & Mensing PC, Houston, TX, argued for plaintiff-appellant. Represented by AMIR H. ALAVI, IFTIKAHR AHMED, ALISA A. LIPSKI.

DARYL JOSEFFER, King & Spalding LLP, Washington, DC, argued for defendant-appellee. Represented by AMELIA GRACE YOWELL; JONATHAN K. WALDROP, MARCUS BARBER, JOHN WALTER DOWNING, DARCY L. JONES, Kasowitz, Benson, Torres & Friedman LLP, Redwood Shores, CA; DAN L. BAGATELL, Perkins Coie LLP, Hanover, NH.

Judges: Before REYNA, BRYSON, and STOLL, Circuit Judges.

Opinion by: STOLL

Opinion

[*1002] STOLL, *Circuit Judge*.

Data Engine Technologies LLC ("DET") appeals the district court's entry of judgment on the pleadings holding that the asserted claims of DET's U.S. Patent Nos. 5,590,259; 5,784,545; 6,282,551; and 5,303,146 are ineligible under *35 U.S.C. § 101*. The district court held that the asserted claims are directed to abstract ideas and fail to provide an inventive concept. We conclude that, with the exception of claim 1 of the '551 patent, the asserted claims of the '259, '545, and '551 patents ("Tab Patents") are directed to patent-eligible subject matter. These claims are **[**2]** not abstract, but rather are directed to a specific improved method for navigating through complex three-dimensional electronic spreadsheets. We agree, however, that the asserted claims of the '146 patent, reciting methods for tracking changes to data in spreadsheets, are directed to the abstract idea of collecting, recognizing, and storing changed information. After a searching review, we find nothing in these claims that provides an inventive concept sufficient to render the claims patent eligible. Accordingly, we affirm-in-part, reverse-in-part, and remand.

BACKGROUND

I. The Tab Patents

The Tab Patents are titled "System and Methods for Improved Spreadsheet Interface With User-Familiar Objects," and claim priority to April 8, 1992.[1] The Tab Patents claim systems and methods for making complex electronic spreadsheets more accessible by providing familiar, user-friendly interface objects—specifically, notebook tabs—to navigate through spreadsheets while circumventing the arduous process of searching for, memorizing, and entering complex commands.

The Tab Patents teach that the advent of electronic spreadsheets offered dramatic improvements in creating, editing, and using spreadsheets to organize **[**3]** and process data. Despite such advantages, twenty-five years ago, electronic spreadsheets were not easy to use. '259 patent col. 2 ll. 57-59. Users were required to master complex commands in order to perform basic operations within a spreadsheet. *Id.* at col. 2 ll. 28-29. To find an appropriate command for an operation, users would navigate through complex menu systems, with the proper command buried under several menus. *Id.* at col. 2 ll. 29-32. "Finding this approach to be unworkable, many users [would] memorize frequently-needed commands instead." *Id.* at col. 2 ll. 41-42. Because such commands were arbitrary (e.g., "/Worksheet Global Default Other International"), users could only master a very small fraction of available commands and features. *Id.* at col. 2 ll. 40-47, 53-56.

The Tab Patents specifically identify problems with navigation through prior art three-dimensional or multipage electronic spreadsheets. The Tab Patents explain that the complex commands required to manipulate each additional spread of the three-dimensional spreadsheet diminished the utility and ease of use of this technology.

[*1003] The invention claimed in the Tab Patents provided a solution to this problem. Specifically, the **[**4]** Tab Patents are directed to and claim a method of implementing a notebook-tabbed interface,

[1] Because the Tab Patents' specifications are substantially identical, we refer only to the '259 patent's specification.

which allows users to easily navigate through three-dimensional electronic spreadsheets. As shown in Figure 4G of the '259 patent below, the Tab Patents provide "an electronic spreadsheet system includ[ing] a notebook interface having a plurality of notebook pages, each of which contains a spread of information cells, or other desired page type." *Id.* at col. 3 ll. 48-52. In contrast to conventional electronic spreadsheets, the method claimed in the Tab Patents "includes user-familiar objects, i.e., paradigms of real-world objects which the user already knows how to use" such as notebook tabs. *Id.* at col. 6 ll. 52-58. "In this manner, complexities of the system are hidden under ordinary, everyday object metaphors," providing a "highly intuitive interface—one in which advanced features (e.g., three-dimensionality) are easily learned." *Id.* at col. 6 ll. 58-63.

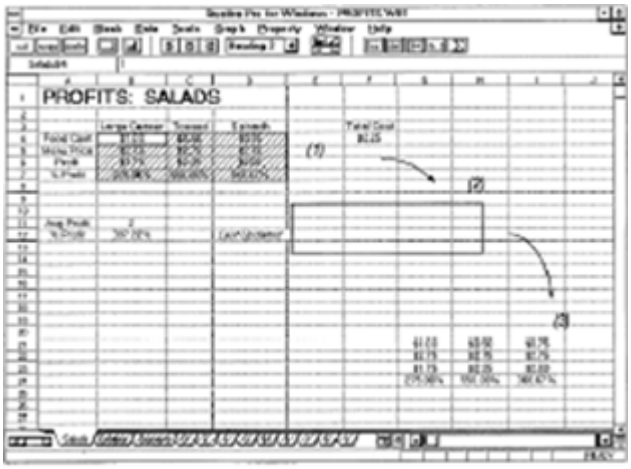


FIG. 4G

Figure 2D below shows more closely an individual spreadsheet page with notebook tabs located along the bottom edge of the page.

FIG. 2D

In this preferred embodiment, "each page identifier is in the form of a tab member (e.g., members 261a, 262a, 263a) situated **[**5]** along a bottom edge of the notebook." *Id.* at col. 8 ll. 13-15. Although these tabs are labeled A, B, and C, etc., they are typically given descriptive names assigned by the user. *Id.* at col. 8 ll. 19-23. To move to different spreadsheet pages, the user selects the corresponding tab for that page. *Id.* at col. 8 ll. 45-47. Thus, **[*1004]** "instead of finding information by scrolling different parts of a large spreadsheet, or by invoking multiple windows of a conventional three-dimensional spreadsheet, the present invention allows the user to simply and conveniently 'flip through' several pages of the notebook to rapidly locate information of interest." *Id.* at col. 8 ll. 51-57. This improved interface allows for "rapidly accessing and processing information on the different pages, including, for example, displaying a plurality of page identifiers for selecting individual pages." *Id.* at col. 3 ll. 53-56.

Although these spreadsheet interfaces have become ubiquitous, Quattro Pro, the first commercial embodiment of the claimed invention, was highly acclaimed as having revolutionized three-dimensional electronic spreadsheets. During prosecution, DET submitted contemporaneous articles showing the state **[**6]** of the art at the time of the invention and evidencing the significance of the claimed methods to spreadsheet technology. For example, *PC World*, a leading computer magazine, published a front-page article, "*Quattro Pro for Windows: The Ultimate 3-D Spreadsheet*." J.A. 981. The article reflected the industry's view that "keeping large, complex worksheet projects organized, manageable, and reliable ha[d] long been a major concern for serious spreadsheet users" and that existing spreadsheets had "data and results hidden all over the place." J.A. 982. The article touts the claimed notebook-tabbed spreadsheet interface as a solution to that problem, explaining that it "makes developing nifty applications far easier for the average spreadsheet user, and [that] intelligent command organization makes navigation efficient." *Id. PC World* published another cover story naming Quattro Pro "The Best of 1992," again lauding it as "the first spreadsheet to make three-dimensional modeling an accessible, useful analytic tool." J.A. 1007. The article stated that "[o]ne of the keys to the product's success is a notebook metaphor, in which each worksheet page can be assigned a descriptive name and users **[**7]** can navigate through the set by clicking on page tabs." *Id.*

Similarly, in 1992, *InfoWorld* named Quattro Pro the product of the year for productivity applications. In doing so, *InfoWorld* wrote:

> We collected all the word processors, spreadsheets, databases, personal information managers, and other productivity applications and asked ourselves a question: "Which of these programs really changed the way an individual user goes about handling data? Does any one stand out as a productivity booster?"
>
> Our answer was Quattro Pro for Windows. The reason: Borland designed this program from the ground up and examined how spreadsheet users would work in a Windows environment. *The*

> *notebook metaphor, with pages and tabs for different worksheets, simplifies handling large worksheets*. The "interface builder" lets a user design custom dialog boxes without extensive macro programming. And, of course, Quattro Pro's graphics are stellar.

J.A. 1008 (emphasis added). In total, DET submitted seven articles dated between 1992 and 1993, all touting the advantages of its use of notebook tabs to improve navigation through three-dimensional spreadsheets. *See* J.A. 981-1010.

DET filed suit against Google LLC, asserting **[**8]** claims 1-2, 12-13, 16-17, 19, 24, 46-47, and 51 of the '259 patent; claims 1-2, 5-7, 10, 13, and 35 of the '545 patent; and claims 1, 3, 6-7, 10, 12-13, 15, and 18 of the '551 patent. The district court considered claim 12 of the '259 patent representative of all asserted claims of the Tab Patents. *See* [Data Engine Techs. LLC v. **[*1005]** Google Inc., 211 F. Supp. 3d 669, 677-78 (D. Del. 2016)] ("*District Court Op.*"). Claim 12 of the '259 patent recites:

> 12. In an electronic spreadsheet system for storing and manipulating information, a computer-implemented method of representing a three-dimensional spreadsheet on a screen display, the method comprising:
>
> displaying on said screen display a first spreadsheet page from a plurality of spreadsheet pages, each of said spreadsheet pages comprising an array of information cells arranged in row and column format, at least some of said information cells storing user-supplied information and formulas operative on said user-supplied information, each of said information cells being uniquely identified by a spreadsheet page identifier, a column identifier, and a row identifier;
>
> while displaying said first spreadsheet page, displaying a row of spreadsheet page identifiers along one side of said first spreadsheet page, each said spreadsheet page identifier being displayed as an image of a notebook **[**9]** tab on said screen display and indicating a single respective spreadsheet page, wherein at least one spreadsheet page identifier of said displayed row of spreadsheet page identifiers comprises at least one user-settable identifying character;
>
> receiving user input for requesting display of a second spreadsheet page in response to selection with an input device of a spreadsheet page identifier for said second spreadsheet page;
>
> in response to said receiving user input step, displaying said second spreadsheet page on said screen display in a manner so as to obscure said first spreadsheet page from display while continuing to display at least a portion of said row of spreadsheet page identifiers; and
>
> receiving user input for entering a formula in a cell on said second spreadsheet page, said formula including a cell reference to a particular cell on another of said spreadsheet pages having a particular spreadsheet page identifier comprising at least one user-supplied identifying character, said cell reference comprising said at least one user-supplied identifying character for said particular spreadsheet page identifier together with said column identifier and said row identifier for said particular **[**10]** cell.

'259 patent col. 26 l. 43—col. 27 l. 17.

II. The '146 Patent

The '146 patent is titled "System and Methods for Improved Scenario Management in an Electronic Spreadsheet." The '146 patent is directed to methods that allow electronic spreadsheet users to track their changes. The specification teaches that prior art electronic spreadsheets were not particularly adept at managing "what-if " scenarios in a given spreadsheet. '146 patent col. 2 ll. 41-44. The patent explains that "[s]ince a given spreadsheet model is routinely created under a set of assumptions (e.g., level of sales, corporate tax rate, and the like), it is desirable to test the extremes of one's assumptions to ascertain the likely results." *Id.* at col. 2 ll. 45-49. Prior art spreadsheets, however, "provided little or no tools for creating and managing such a multitude of scenarios." *Id.* at col. 2 ll. 51-52. Instead, users had to "resort to manually creating separate copies of the underlying model, with the user responsible for tracking any modifications made in the various copies." *Id.* at col. 2 ll. 53-56.

The '146 patent purports to solve this problem by providing an electronic spreadsheet system "having a preferred interface and methods for creating and tracking various **[*1006]** versions or **[**11]** 'scenarios' of a data model." *Id.* at col. 2 ll. 61-63. The claimed system "includes tools for specifying a 'capture area,' that is, a specific set of information cells to be tracked and an Identify Scenario tool for automatically determining changes between a captured parent or baseline model and a new scenario." *Id.* at col. 2 ll. 63-67.

DET alleged infringement of claims 1, 26-28, and 32-34 of the '146 patent. The district court considered independent claims 1 and 26 representative of all the asserted claims of the '146 patent. *See* District Court Op., 211 F. Supp. 3d at 680. Claims 1 and 26 recite:

1. In an electronic spreadsheet system for modeling user-specified information in a data model comprising a plurality of information cells, a method for automatically tracking different versions of the data model, the method comprising:

> (a) specifying a base set of information cells for the system to *track changes*;
> (b) creating a new version of the data model by modifying at least one information cell from the specified base set; and
> (c) automatically determining cells of the data model which have changed by comparing cells in the new version against corresponding ones in the base set.
> ***
>
> 26. In an electronic spreadsheet system, a method for storing different **[**12]** versions of a spreadsheet model, the method comprising:
> (a) maintaining a base version of the spreadsheet model as ordered information on a storage device; and
> (b) for each new version of the spreadsheet model:
> (i) determining portions of the new version which have changed when compared against the base version, and
> (ii) maintaining the new version by storing additional information for only those portions determined to have changed.

'146 patent col. 14 ll. 1-13 (emphasis added), col. 16 ll. 7-19.

III. The District Court's Decision

Google filed a motion for judgment on the pleadings under Federal Rule of Civil Procedure 12(c), arguing that the asserted claims of the Tab Patents and the '146 patent are directed to patent-ineligible subject matter under *§ 101*. The district court granted the motion with respect to the Tab Patents, concluding that representative claim 12 of the '259 patent is "directed to the abstract idea of using notebook-type tabs to label and organize spreadsheets." District Court Op., 211 F. Supp. 3d at 678. The district court also agreed with Google that claim 12 "is directed to an abstract idea that humans have commonly performed entirely in their minds, with the aid of columnar pads and writing instruments." *Id. at 679*. The district court held that the remaining limitations of claim 12 fail to **[**13]** recite an inventive concept. *Id.*

Similarly, with respect to the '146 patent, the district court concluded that the asserted claims are directed to the abstract idea of "collecting spreadsheet data, recognizing changes to spreadsheet data, and storing information about the changes," and more specifically, directed "to input of information in a (computerized) columnar pad, recognition of changes in later versions of the inputted information, and storage of information about the changes." *Id. at 680-81* (emphases omitted). The district court also held that additional claim limitations directed to electronic spreadsheets failed to provide an inventive concept sufficient to confer patent eligibility. *Id.*

DET appeals. We have jurisdiction pursuant to *28 U.S.C. § 1295(a)(1)*.

[*1007] DISCUSSION

I

HN1[↑] We review the district court's judgment on the pleadings under regional circuit law. *Merck & Co. v. Hi-Tech Pharmacal Co., 482 F.3d 1317, 1320 (Fed. Cir. 2007)*. The Third Circuit reviews the grant of judgment on the pleadings de novo, "accept[ing] all of the allegations in the pleadings of the party against whom the motion is addressed as true and draw[ing] all reasonable inferences in favor of the non-moving party." *Allstate Prop. & Cas. Ins. Co. v. Squires, 667 F.3d 388, 390 (3d Cir. 2012)*. Patent eligibility can be determined on the pleadings under *Rule 12(c)* when there are no factual allegations that, when taken **[**14]** as true, prevent resolving the eligibility question as a matter of law. *Cf. Aatrix Software, Inc. v. Green Shades Software, Inc., 882 F.3d 1121, 1125 (Fed. Cir. 2018)*; *Berkheimer v. HP Inc., 881 F.3d 1360, 1365 (Fed. Cir. 2018)*.

HN2[↑] *Section 101* provides that "[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor." *35 U.S.C. § 101*. In *Alice Corp. v. CLS Bank International*, the Supreme Court articulated a two-step test for examining patent eligibility under *§ 101*. *134 S. Ct. 2347, 82 L. Ed. 2d 296, 189 L. Ed. 2d 296 (2014)*. "We must first determine whether the claims at issue are directed to a patent-ineligible concept." *Id. at 2355*. "Laws of nature, natural phenomena, and abstract ideas

are not patentable." *Id. at 2354* (quoting *Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576, 589, 133 S. Ct. 2107, 186 L. Ed. 2d 124 (2013)*). "The 'abstract ideas' category embodies 'the longstanding rule that '[a]n idea of itself is not patentable.'" *Id. at 2355* (alteration in original) (quoting *Gottschalk v. Benson, 409 U.S. 63, 67, 93 S. Ct. 253, 34 L. Ed. 2d 273 (1972)*). If the claims are not directed to a patent-ineligible concept under *Alice* step 1, "the claims satisfy *§ 101* and we need not proceed to the second step." *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc., 880 F.3d 1356, 1361 (Fed. Cir. 2018)* (citing *Visual Memory LLC v. NVIDIA Corp., 867 F.3d 1253, 1262 (Fed. Cir. 2017)*).

If the claims are directed to a patent-ineligible concept, however, we next consider *Alice* step two. ***HN3***[↑] In this step, we consider "the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible **[**15]** application." *Alice, 134 S. Ct. at 2355* (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 78-79, 132 S. Ct. 1289, 182 L. Ed. 2d 321 (2012)*). This second step is "a search for an 'inventive concept'—*i.e.*, an element or combination of elements that is 'sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.'" *Id.* (alteration in original) (quoting *Mayo, 566 U.S. at 72-73*).

II

We first address the Tab Patents. Our analysis begins at *Alice* step one, asking "whether the claims at issue are directed to a patent-ineligible concept." *Id. at 2355*. With the exception of claim 1 of the '551 patent, we hold that the asserted claims of the Tab Patents are directed to patent-eligible subject matter.

A

When considered as a whole, and in light of the specification, representative claim 12 of the '259 patent is not directed to an abstract idea. Rather, the claim is **[*1008]** directed to a specific method for navigating through three-dimensional electronic spreadsheets. The method provides a specific solution to then-existing technological problems in computers and prior art electronic spreadsheets. The specification teaches that prior art computer spreadsheets were not user friendly. They required users to "master many complex and arbitrary operations." '259 patent col. 2 ll. 28-29. Users had to search through complex **[**16]** menu systems to find appropriate commands to execute simple computer tasks, which required users to memorize frequently needed commands. *Id.* at col. 2 ll. 29-45. This was burdensome and hindered a user's ability to find or access the many commands and features available in prior art computer spreadsheets, undercutting the effectiveness of the computer as a means to review and edit a spreadsheet. *Id.* at col. 2 ll. 45-56. This was particularly true for three-dimensional spreadsheets, which allowed users to build spreadsheet workspaces consisting of multiple two-dimensional spreadsheets, further increasing the complexity of using and navigating between multiple spreadsheets. *Id.* at col. 2 l. 66-col. 3 l. 24.

The Tab Patents solved this known technological problem in computers in a particular way—by providing a highly intuitive, user-friendly interface with familiar notebook tabs for navigating the three-dimensional worksheet environment. *Id.* at col. 3 ll. 44-52. The improvement allowed computers, for the first time, to provide rapid access to and processing of information in different spreadsheets, as well as easy navigation in three-dimensional spreadsheets. The invention was applauded **[**17]** by the industry for improving computers' functionality as a tool able to instantly access all parts of complex three-dimensional electronic spreadsheets. Numerous contemporaneous articles attributed the improved three-dimensional spreadsheets' success to its notebook tab feature.[2]

Representative claim 12 recites precisely this technical solution and improvement in computer spreadsheet functionality. The claim recites specific steps detailing

---

[2] The district court declined to consider the articles included in the prosecution history, relying only on the pleadings and the patents attached to DET's complaint. *District Court Op., 211 F. Supp. 3d at 681 n.4*. ***HN4***[↑] On a motion for judgment on the pleadings, however, the court may consider "matters of public record." *Cf. Bruni v. City of Pittsburgh, 824 F.3d 353, 360 (3d Cir. 2016)* (quoting *Pension Benefit Guar. Corp. v. White Consol. Indus., Inc., 998 F.2d 1192, 1196 (3d Cir. 1993)*). Prosecution histories constitute public records. *See Hockerson-Halberstadt, Inc. v. Avia Group Int'l, Inc., 222 F.3d 951, 957 (Fed. Cir. 2000)* ("The prosecution history constitutes a public record . . . ."); *see 37 C.F.R. § 1.11(a)* ("The specification, drawings, and all papers to the file of: [a] published application; a patent; or a statutory invention registration are open to inspection by the public . . . ."). We consider this evidence relevant in our de novo review because it is part of the Tab Patents' prosecution histories and was relied on in DET's opposition to Google's *Rule 12(c)* motion.

the method of navigating through spreadsheet pages within a three-dimensional spreadsheet environment using notebook tabs. The claim requires displaying on a screen display a row of spreadsheet page identifiers along one side of the first spreadsheet page, with each spreadsheet page identifier being a notebook tab. The claim requires at least one user-settable identifying character to label the notebook tab and describes navigating through the various spreadsheet pages through selection of the notebook tabs. The claim further requires a formula that uses the identifying character to operate on information spread between different spreadsheet pages that are identified by their tabs. The claimed method does not recite the idea of navigating **[**18]** through spreadsheet pages using buttons or a generic method of labeling and **[*1009]** organizing spreadsheets. Rather, the claims require a specific interface and implementation for navigating complex three-dimensional spreadsheets using techniques unique to computers.

In this regard, claim 12 is similar to the claims we held patent eligible in *Core Wireless*. There, the claims were directed to an improved display interface that allowed users to more quickly access stored data and programs in small-screen electronics, thereby improving the efficient functioning of the computer. *Core Wireless, 880 F.3d at 1359*. The prior art taught that small-screen electronic interfaces required users to scroll through and switch views to find desired data and functions. *Id. at 1363*. Core Wireless's invention, however, improved the efficiency of these display interfaces. By displaying only a limited list of common functions and data from which to choose, the invention spared users from time-consuming operations of navigating to, opening up, and then navigating within, each separate application. *Id.* The invention thus increased the efficiency with which users could navigate through various views and windows. *Id.* We rejected the accused infringer's contention **[**19]** that the claims were merely directed to the abstract idea of indexing information because the claims were directed "to an improved user interface for computing devices" and "a *particular* manner of summarizing and presenting information in electronic devices." *Id. at 1362* (emphasis added). We concluded that the claims were patent eligible because the claims "recite[d] a specific improvement over prior systems, resulting in an improved user interface for electronic devices," and thus were directed to "an improvement in the functioning of computers." *Id. at 1363*.

Claim 12 of the '259 patent similarly recites a method that differs from prior art navigation methods and "provide[s] for rapidly accessing and processing information" in three-dimensional spreadsheets. '259 patent col. 3 ll. 53-54. "[I]nstead of finding information by scrolling different parts of a large spreadsheet" the invention "allows the user to simply and conveniently 'flip through' several pages of the notebook to rapidly locate information of interest." *Id.* at col. 8 ll. 51-57. Moreover, akin to the claims in *Core Wireless*, claim 12 recites a "specific" and "particular" manner of navigating a three-dimensional spreadsheet that improves the efficient functioning **[**20]** of computers. *See Core Wireless, 880 F.3d at 1362, 1363*.

Likewise, claim 12 comports with the claims we held patent eligible in *Trading Technologies International, Inc. v. CQG, Inc. 675 F. App'x 1001 (Fed. Cir. 2017)*. There, the claims recited a trading system in which a graphical user interface displayed dynamic bid and ask prices for a particular commodity traded in the market along with a static display of prices corresponding to the bids and asks. *Id. at 1003*. The system paired orders with the static display of prices to prevent entry of orders that had changed prices. *Id.* The patents explained that the invention solved an existing problem in the prior art by reducing the time it took to place and execute a trading order. We agreed with the district court that "the challenged patents 'solve[d] problems of prior graphical user interface devices . . . in the context of computerized trading[] relating to speed, accuracy and usability.'" *Id. at 1004* (alterations in original) (quoting *Trading Techs. Int'l, Inc. v. CQG, Inc., No. 05-cv-4811, 2015 U.S. Dist. LEXIS 22039, 2015 WL 774655, at *4 (N.D. Ill. Feb. 24, 2015)*). As the district court had explained, the claims were not merely directed to displaying information on a graphical user interface, but rather "require[d] a specific, structured graphical user interface paired with a prescribed functionality directly related to the graphical user interface's **[**21]** structure **[*1010]** that is addressed to and resolves a specifically identified problem in the prior state of the art." *Id.* We agreed and adopted the district court's articulated reasons to conclude that the claims were not abstract under *Alice* step one. *Id.*

Google asserts that this court has repeatedly found that claims directed to methods of organizing and presenting information are abstract and that we should so hold here. During oral argument, Google identified three cases to best support its position: *Affinity Labs of Texas, LLC v. DirecTV, LLC, 838 F.3d 1253 (Fed. Cir. 2016)*; *Intellectual Ventures I LLC v. Capital One Financial Corp., 850 F.3d 1332 (Fed. Cir. 2017)* (hereinafter, "*Capital One*"); and *Intellectual Ventures I LLC v. Erie*

Indemnity Co., 850 F.3d 1315 (Fed. Cir. 2017) (hereinafter, "*Erie Indemnity*"). *See* Oral Arg. at 29:57-30:51, http://oralarguments.cafc.uscourts.gov/default.aspx?fl=2017-1135.mp3. We have reviewed these cases, but conclude that the claims in those cases were materially different.

In *Affinity Labs*, we held that claims directed to "streaming regional broadcast signals to cellular telephones located outside the region" were ineligible because "[t]he concept of providing out-of-region access to regional broadcast content is an abstract idea." *838 F.3d at 1255, 1258*. The claims were "entirely functional in nature," and we found nothing in the claims "directed to *how* to implement out-of-region broadcasting." *Id. at 1258*. Although the representative claim **[**22]** also recited "a graphical user interface" for displaying a menu of available media options from which a user could select, the limitation was "conventional," insignificant extra-solution activity and thus insufficient to confer patent eligibility. *Id. at 1261*. In *Capital One*, the claims were directed to an apparatus for managing eXtensible Markup Language ("XML") documents. *850 F.3d at 1338*. The invention allowed users to make changes to data in a "dynamic document," which could then be dynamically propagated back into an original XML document. *Id. at 1339*. We held those claims were "directed to the abstract idea of collecting, displaying, and manipulating data." *Id. at 1340*. In *Erie Indemnity*, we held that claims reciting a method for searching a database using an index of descriptive terms associated with "category" and "domain" tags were directed to the abstract idea of "creating an index and using that index to search for and retrieve data." *850 F.3d at 1326-27*. The claims did not recite any specific structure or improvement of computer functionality sufficient to render the claims not abstract. *Id. at 1328-29*.

In contrast to *Affinity Labs, Capital One*, and *Erie Indemnity*, representative claim 12 is not simply directed to displaying a graphical user interface **[**23]** or collecting, manipulating, or organizing information to improve navigation through three-dimensional spreadsheets.[3] Instead, the claim recites **[*1011]** a specific structure (i.e., notebook tabs) within a particular spreadsheet display that performs a specific function (i.e., navigating within a three-dimensional spreadsheet).

Nor is representative claim 12 directed generally to displaying information on a screen, without "requir[ing] a new source or type of information, or new techniques for analyzing it," like the claims in *Electric Power Group, LLC v. Alstom S.A. 830 F.3d 1350, 1353-54 (Fed. Cir. 2016)*. And unlike ineligible claims that merely "collect[], organiz[e], and display . . . information on a generic display device," claim 12 recites "a specific improvement to the way computers . . . operate." *See Interval Licensing LLC v. AOL, Inc., 896 F.3d 1335, 1345 (Fed. Cir. 2018)* (quoting *Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1336 (Fed Cir. 2016))*.

HN5[] At *Alice* step one, "it is not enough to merely identify a patent-ineligible concept underlying the claim; we must determine whether that patent-ineligible concept is what the claim is 'directed to.'" *Rapid Litig. Mgmt. Ltd. v. CellzDirect, Inc., 827 F.3d 1042, 1050 (Fed. Cir. 2016)*. And that inquiry requires that the claims be read as a whole. *See Alice, 134 S. Ct. at 2355 n.3*. We conclude that, when read as a whole, in light of the specification, claim 12 is directed to more than a generic or abstract idea as it claims a particular manner of navigating three-dimensional **[**24]** spreadsheets, implementing an improvement in electronic spreadsheet functionality.

Google avers that humans have long used tabs to organize information. It cites tabbed notebooks, binder dividers, file folders, and sticky Post-it notes as well-known examples of organizing information using tabs. We agree that tabs existed outside the context of electronic spreadsheets prior to the claimed invention. It is not enough, however, to merely trace the invention to some real-world analogy. The eligibility question is not whether anyone has ever used tabs to organize

---

[3] We have also considered *Affinity Labs of Texas, LLC v. Amazon.com Inc., 838 F.3d 1266 (Fed. Cir. 2016)*, also cited by Google, and find it distinguishable as well. There, the claims were directed to "a network-based media system with a customized user interface, in which the system delivers streaming content from a network-based resource." *Id. at 1268*. We held the claims ineligible because "the concept of delivering user-selected media content to portable devices is an abstract idea." *Id. at 1269*. Although the claim recited a "customized user interface," we held that "'customizing information based on . . . information known about the user' is an abstract idea." *Id. at 1271* (alteration in original) (quoting *Intellectual Ventures I LLC v. Capital One Bank (USA), 792 F.3d 1363, 1369 (Fed. Cir. 2015))*. Representative claim 12 of the '259 patent, however, is different. Although its recited notebook tabs can be customized, *see* '259 patent col. 8 ll. 19-23, they are more than merely labeled tabs. They implement a specific function—an improved manner of navigating through the spreadsheet.

information. That question is reserved for §§ 102 and 103. HN6[] The question of abstraction is whether the claim is "directed to" the abstract idea itself. *Id.* We must consider the claim as a whole to determine whether the claim is directed to an abstract idea or something more. Google fails to appreciate the functional improvement achieved by the specifically recited notebook tabs in the claimed methods. The notebook appearance of the tabs was specifically chosen by the inventors because it is easily identified by users. The tabs are not merely labeled buttons or other generic icons. DET has disclaimed as much. *See* Oral Arg. at 11:03-47. Rather, **[**25]** the notebook tabs are specific structures within the three-dimensional spreadsheet environment that allow a user to avoid the burdensome task of navigating through spreadsheets in separate windows using arbitrary commands.

Because we conclude that representative claim 12 of the '259 patent is not abstract under *Alice* step one, we need not reach *Alice* step two with respect to claim 12. *See* Core Wireless, 880 F.3d at 1363.

B

Notwithstanding our conclusion that representative claim 12 of the '259 patent is directed to patent-eligible subject matter, we conclude that claim 1 of the '551 patent is ineligible.

Claim 1 of the '551 patent recites:

> 1. In an electronic spreadsheet for processing alphanumeric information, said . . . electronic spreadsheet comprising a three-dimensional spreadsheet operative in a digital computer and including a plurality **[*1012]** of cells for entering data and formulas, a method for organizing the three-dimensional spreadsheet comprising:
> partitioning said plurality of cells into a plurality of two-dimensional cell matrices so that each of the two-dimensional cell matrices can be presented to a user as a spreadsheet page;
>
> associating each of the cell matrices with a user-settable page identifier which serves as a unique identifier for said each cell **[**26]** matrix;
> creating in a first cell of a first page at least one formula referencing a second cell of a second page said formula including the user-settable page identifier for the second page; and
> storing said first and second pages of the plurality of cell matrices such that they appear to the user as being stored within a single file.

'551 patent col. 23 l. 60—col. 24 l. 13.

We conclude that under *Alice* step one, this claim is directed to the abstract idea of identifying and storing electronic spreadsheet pages. DET concedes that, unlike claim 12 of the '259 patent, claim 1 of the '551 patent is "directed at something a bit more general." *See* Oral Arg. at 9:55-58. Indeed, it generically recites "associating each of the cell matrices with a user-settable page identifier" and does not recite the specific implementation of a notebook tab interface. '551 patent col. 24 ll. 3-4. Claim 1 of the '551 patent is therefore not limited to the specific technical solution and improvement in electronic spreadsheet functionality that rendered representative claim 12 of the '259 patent eligible. Instead, claim 1 of the '551 patent covers any means for identifying electronic spreadsheet pages.

Because claim 1 of the '551 patent is directed to an abstract idea, we must turn to *Alice* step two **[**27]** to "determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." Alice, 134 S. Ct. at 2355 (quoting Mayo, 566 U.S. at 78). HN7[] The "mere recitation of a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." Id. at 2358. "For the role of a computer in a computer-implemented invention to be deemed meaningful in the context of this analysis, it must involve more than performance of 'well-understood, routine, [and] conventional activities previously known to the industry.'" Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n, 776 F.3d 1343, 1347-48 (Fed. Cir. 2014) (alteration in original) (quoting Alice, 134 S. Ct. at 2359).

After a searching review, the additional elements of claim 1 of the '551 patent fail to provide an inventive concept. Claim 1 merely recites partitioning cells to be presented as a spreadsheet, referencing in one cell of a page a formula referencing a second page, and saving the pages such that they appear as being stored as one file. These limitations merely recite the method of implementing the abstract idea itself and thus fail under *Alice* step two. Therefore, we conclude that claim 1 of the '551 patent is ineligible under *§ 101*.

III

Finally, we turn to the '146 patent, which is directed to a method of tracking changes in three-dimensional spreadsheets. Beginning at *Alice* step **[**28]** one, we agree with the district court that these claims are directed to the abstract idea of collecting spreadsheet

data, recognizing changes to spreadsheet data, and storing information about the changes.

The district court considered claims 1 and 26 representative of all asserted **[*1013]** claims of the '146 patent. *See* District Court Op., 211 F. Supp. 3d at 680. At their core, these claims recite tracking changes in a spreadsheet by: (1) creating a base version of a spreadsheet, (2) creating a new version of the spreadsheet, and (3) determining which cells of data have changed by comparing the new and base versions. The concept of manually tracking modifications across multiple sheets is an abstract idea. The mere automation of this process does not negate its abstraction. Unlike claim 12 of the '259 patent, nothing in the '146 patent's claims viewed in light of the specification convinces us that the claimed method improves spreadsheet functionality in a specific way sufficient to render the claims not abstract.

We agree with the district court that these claims are akin to those we held ineligible in *Content Extraction*. There, the claims were directed to methods of extracting data from hard-copy documents using an automated scanner, recognizing information from **[**29]** the extracted data, and storing that data in memory. *Content Extraction, 776 F.3d at 1345, 1347*. We see no material difference in the level of abstraction here. The '146 patent's claims recite determining changes to spreadsheets by comparing the cells in two versions of the spreadsheet and storing that information. We reject DET's attempt to distinguish *Content Extraction* on the ground that it involved a business method. Regardless of the field of the technology, the claims at issue here are sufficiently similar to those in *Content Extraction* for us to conclude that the claims of the '146 patent are also abstract. As in *Content Extraction*, we hold that the asserted claims of the '146 patent are directed to the abstract idea of collecting, recognizing, and storing the recognized data in memory. *Id. at 1347*.

We also conclude that the asserted claims of the '146 patent do not recite an inventive concept under *Alice* step two. The claims recite the generic steps of creating a base version of a spreadsheet, creating a new version of the spreadsheet, and determining changes made to the original version. These claims do not recite anything "more than simply stat[ing] the [abstract idea] while adding the words 'apply it.'" *Alice, 134 S. Ct. at 2357* (alterations in original) (quoting *Mayo, 566 U.S. at 72*). "[T]he mere recitation of **[**30]** a generic computer cannot transform a patent-ineligible abstract idea into a patent-eligible invention." *Id. at 2358*. We have considered DET's arguments that other claims of the '146 patent, including claims 27 and 28, provide an additional inventive concept and find them unpersuasive.

CONCLUSION

For the foregoing reasons, we conclude that, with the exception of claim 1 of the '551 patent, the asserted claims of the Tab Patents are not directed to patent-ineligible subject matter under *Alice* step one and therefore satisfy *§ 101*. We determine, however, that the asserted claims of the '146 patent are directed to an abstract idea, provide no inventive concept, and are therefore ineligible under *§ 101*.

AFFIRMED-IN-PART, REVERSED-IN-PART, AND REMANDED

COSTS

No costs.

End of Document

Seven Networks, LLC v. Google LLC

United States District Court for the Eastern District of Texas, Marshall Division

July 19, 2018, Decided; July 19, 2018, Filed

CIVIL ACTION NO. 2:17-CV-00442-JRG

Reporter
315 F. Supp. 3d 933 *; 2018 U.S. Dist. LEXIS 176265 **

SEVEN NETWORKS, LLC, Plaintiff, v. GOOGLE LLC, Defendant.

Subsequent History: Writ denied by *In re Google LLC, 2018 U.S. App. LEXIS 31000 (Fed. Cir., Oct. 29, 2018)*

Prior History: *Seven Networks, LLC v. Google LLC, 2018 U.S. Dist. LEXIS 112210 (E.D. Tex., July 6, 2018)*

Core Terms

Google, servers, infringement, place of business, regular, venue, established place of business, warehouse, patent, space, network, Edge, requirements, Host, Cache, Dictionary, Nodes, users, vending machine, business', services, statutory language, venue statute, proper venue, courts, customers, parties, lease, centers, Amazon

Counsel: **[**1]** For Seven Networks, Llc, Plaintiff: Adrienne Elizabeth Dominguez, Austin Chun Teng, Herbert J Hammond, James Michael Heinlen, Justin S. Cohen, Massimo Ciccarelli, Matthew William Cornelia, Nadia Elena Haghighatian, Natalie Marguerite Cooley, Richard Lawrence Wynne, Jr, Vishal Hemant Patel, Bruce S Sostek, Thompson & Knight LLP - Dallas, Dallas, TX USA; Eric Sorensen Hansen, Erik Bruce Fountain, Samuel Franklin Baxter, Theodore Stevenson, III, McKool Smith PC - Dallas, Dallas, TX USA; Jennifer Leigh Truelove, McKool Smith - Marshall, Marshall, TX USA.

For Google Llc, Defendant: Charles Kramer Verhoeven, LEAD ATTORNEY, Brian E Mack, Felipe Corredor, Jonathan Tse, Lindsay M Cooper, Michael D. Yoo, Sean S Pak, Quinn Emanuel Urquhart & Sullivan LLP - San Francisco, San Francisco, CA USA; Andrea Pallios Roberts, Quinn Emanuel Urquhart & Sullivan LLP - Redwood, Redwood Shores, CA USA; Erika Hart Warren, Matthew S Warren, Warren Lex LLP, San Francisco, CA USA; John Frederick Bufe, Michael E Jones, Patrick Colbert Clutter, IV, Potter Minton, a Professional Corporation, Tyler, TX USA Lance Lin Yang, Miles Davenport Freeman, Nithin Kumar, Quinn Emanuel Urquhart & Sullivan, LLP - LA, Los Angeles, **[**2]** CA USA; Patrick Curran, Quinn Emanuel Urquhart & Sullivan, LLP - NY, New York, NY USA; Patrick Aubrey Fitch, Warren Lex LLP - Boston, Boston, MA USA.

For Samsung Electronics Co., Ltd., Consolidated Civil Action 2:17cv441, Consol Defendant: Ruffin B Cordell, LEAD ATTORNEY, Cyrus Garmestani, Indranil Mukerji, Laura C. Whitworth, Michael J McKeon, Ralph A Phillips, Stephen Andrew Marshall, Fish & Richardson PC - Washington DC, Washington, DC USA; C. Noah Graubart, Thad C Kodish, Fish & Richardson PC - Atlanta, Atlanta, GA USA; Leonard Davis, Fish & Richardson P.C. - Dallas, Dallas, TX USA; Linhong Zhang, PRO HAC VICE, Fish & Richardson PC - Washington DC, Washington, DC USA; Melissa Richards Smith, Gillam & Smith, LLP, Marshall, TX USA; William Peter Guarnieri, Fish & Richardson P.C. - DC, Washington, DC USA.

For Samsung Electronics America, Inc., Consolidated Civil Action 2:17cv441, Consol Defendant, Consol Counter Claimant: Ruffin B Cordell, LEAD ATTORNEY, Cyrus Garmestani, Indranil Mukerji, Laura C. Whitworth, Michael J McKeon, Ralph A Phillips, Stephen Andrew Marshall, Sun Young Park, Fish & Richardson PC - Washington DC, Washington, DC USA; C. Noah Graubart, Thad C Kodish, Fish & Richardson **[**3]** PC - Atlanta, Atlanta, GA USA; Leonard Davis, Fish & Richardson P.C. - Dallas, Dallas, TX USA; Linhong Zhang, PRO HAC VICE, Fish & Richardson PC - Washington DC, Washington, DC USA; Melissa Richards Smith, Gillam & Smith, LLP, Marshall, TX USA; William Peter Guarnieri, Fish & Richardson P.C. - DC, Washington, DC USA.

For Samsung Electronics Co., Ltd., Consolidated Civil Action 2:17cv441, Consol Counter Claimant: Ruffin B Cordell, LEAD ATTORNEY, Cyrus Garmestani, Indranil

Mukerji, Laura C. Whitworth, Michael J McKeon, Ralph A Phillips, Stephen Andrew Marshall, Sun Young Park, Fish & Richardson PC - Washington DC, Washington, DC USA; C. Noah Graubart, Thad C Kodish, Fish & Richardson PC - Atlanta, Atlanta, GA USA; Leonard Davis, Fish & Richardson P.C. - Dallas, Dallas, TX USA; Linhong Zhang, PRO HAC VICE, Fish & Richardson PC - Washington DC, Washington, DC USA; Melissa Richards Smith, Gillam & Smith, LLP, Marshall, TX USA; William Peter Guarnieri, Fish & Richardson P.C. - DC, Washington, DC USA.

For Seven Networks, Llc, Consolidated Civil Action 2:17-441, Consol Counter Defendant: Austin Chun Teng, Justin S. Cohen, Massimo Ciccarelli, Natalie Marguerite Cooley, Thompson & Knight LLP - **[**4]** Dallas, Dallas, TX USA; Erik Bruce Fountain, McKool Smith PC - Dallas, Dallas, TX USA; Jennifer Leigh Truelove, McKool Smith - Marshall, Marshall, TX USA.

Judges: RODNEY GILSTRAP, UNITED STATES DISTRICT JUDGE.

Opinion by: RODNEY GILSTRAP

Opinion

[*937] FILED UNDER SEAL

MEMORANDUM OPINION AND ORDER

Before the Court is Google LLC's ("Google") Second Renewed Motion to Dismiss or, in the Alternative, Transfer under *28 U.S.C. § 1406* for Improper Venue. (Dkt. No. 125) ("the Motion"). Having considered the Motion, the Court is of the opinion that it should be **DENIED** for the reasons contained herein.

I. Procedural Background

SEVEN Networks, LLC, ("SEVEN") filed suit against Google on May 17, 2017, alleging, *inter alia*, patent infringement. (Dkt. No. 1). On August 8, 2017, Google filed a Motion to Dismiss under *Rule 12(b)(3)*. (Dkt. No. 25). In response, SEVEN filed the Amended Complaint that is the subject of the present motion. (Dkt. No. 34). On September 12, 2017, Google filed a Renewed Motion to Dismiss ("Second Motion to Dismiss"), again under *Rule 12(b)(3)*. In response, along with its opposition to the Second Motion to Dismiss, SEVEN filed a Contingent Motion for Leave to Conduct Venue Discovery. (Dkt. No. 77).

On December 22, 2017, the Court entered a Venue Discovery **[**5]** Order, which directed the parties to conduct discovery on Google's venue motions by February 22, 2018, and directed Google to refile its venue motions no later than two weeks after the close of venue discovery. (Dkt. No. 107). The Court then granted the Parties' **[*938]** motion to extend venue discovery to March 1, 2018. (Dkt. No. 115). Following the close of venue discovery, Google filed the instant Motion and a related Motion to Transfer Venue to the Northern District of California. (Dkt. Nos. 125, 126). The Court held a hearing on the instant Motion on June 1, 2018. (Dkt. No. 186).

II. Applicable Law

In today's post-*TC Heartland* world, venue law in patent cases continues its development. *See generally* *In re Cray Inc., 871 F.3d 1355 (Fed. Cir. 2017)*; *In re Micron Tech., Inc., 875 F.3d 1091 (Fed. Cir. 2017)*; *In re HTC Corp., 889 F.3d 1349 (Fed. Cir. 2018)*; *In re BigCommerce, Inc., 890 F.3d 978 (Fed. Cir. 2018)*; *In re ZTE (USA) Inc., 890 F.3d 1008 (Fed. Cir. 2018)*; and *In re Intex Recreation Corp.*, No. 2018-131, 2018 WL 3089215 (Fed. Cir. June 13, 2018).

Venue in patent infringement actions is defined by *28 U.S.C. § 1400(b)*. There is no doubt that any analysis of venue under *28 U.S.C. § 1400(b)* "begin[s] with the language of the statute." *In re BigCommerce, 890 F.3d at 982* (citing *Mallard v. U.S. Dist. Court for the S. Dist. of Iowa, 490 U.S. 296, 300, 109 S. Ct. 1814, 104 L. Ed. 2d 318 (1989)*). *Section 1400(b) of Title 28, United States Code* states:

> Any civil action for patent infringement may be brought in the judicial district where the defendant resides, or where the defendant has committed acts of infringement and has a regular and established place of business.

The Federal Circuits' first, and most general, guidance on how a district court should approach **[**6]** this venue statute was provided by *In re Cray. 871 F.3d 1355*. There, the Federal Circuit struck down this Court's suggested test as "not sufficiently tethered to this statutory language" and for "fail[ing] to inform each of the necessary requirements of the statute." *Id. at 1362*. The Circuit continued:

> In deciding whether a defendant has a regular and

> established place of business in a district, no precise rule has been laid down and each case depends on its own facts. The "requirements" listed above and discussed below inform whether there exist the necessary elements, but do not supplant the statutory language. We stress that the analysis must be closely tied to the language of the statute.

Id. Accordingly, district courts must hew closely to an analysis which is guided by the language of the statute.[1]

Beyond this admonition, the Federal Circuit provided additional guidance on what it believed to be the major requirements of the statutory language; these lodestars guide district courts in their application of the statute to case specific facts. Specifically, the Federal Circuit held that "§ 1400(b) requires that 'a defendant has' a 'place of business' that is 'regular' and 'established.' All of these requirements must be **[**7]** present." *Id.* These requirements were further refined: "the first requirement is that there must be a physical place in the district"; "[t]he second requirement . . . is that the place must be a regular and established place of business"; and "the third requirement . . . is that the regular and established place of business must be the place of the defendant." *Id. at 1362-63* (internal quotation marks omitted). Having **[*939]** set forth a three-part test[2] for the application of the statute, the Federal Circuit then examined each identified requirement in greater detail.

As to the requirement that there is a "physical place in the district," the Federal Circuit noted that a "place" is defined as "a building or a part of a building set apart for any purpose or quarters of any kind from which business is conducted." *Id. at 1362* (citing William Dwight Whitney, THE CENTURY DICTIONARY, 4520 (Benjamin E. Smith, ed. 1911); *Place*, BLACK'S LAW DICTIONARY (1st ed. 1891)) (internal quotations omitted). The Federal Circuit further noted that the statute "cannot be read to refer *merely* to a virtual space or to electronic communications from one person to another." *In re Cray, 871 F.3d at 1362* (emphasis added).[3][4][5]

[*940] Turning to the requirement that the place "must be a regular and established place of business," the Federal Circuit has instructed that the place of business must be "regular," by, for example, operating in a "steady, uniform, orderly, and methodical manner." *In re Cray, 871 F.3d at 1362* (cleaned up) (citing THE CENTURY DICTIONARY, *supra*, at 5050). This business may not be temporary or for some special work or particular transaction; a single act does not constitute business, but a series of such acts does. *Id.* (citations

---

[1] *Accord* *In re BigCommerce, 890 F.3d at 985* ("The requirement of venue is specific and unambiguous; it is not one of those vague principles which, in the interest of some overriding policy, is to be given a 'liberal' construction . . . . We cannot ignore the requirements of the statute merely because different requirements may be more suitable for a more modern business environment.") (quoting *Schnell v. Peter Eckrich & Sons, Inc., 365 U.S. 260, 264, 81 S. Ct. 557, 5 L. Ed. 2d 546 (1961)*).

[2] Describing *In re Cray* as setting forth a precise test of any kind likely reads too much into the actions of the Federal Circuit. As noted *supra*, the Circuit specifically held that the "requirements" it provided "inform . . . but do not supplant the statutory language." *Id. at 1362*. Accordingly, *In re Cray* is properly viewed as a set of guidelines. Thus, a district court may rely on *In re Cray* but must be mindful that its first master when determining proper venue is the statute itself.

[3] The Federal Circuit's inclusion of "merely" indicates that a virtual space or electronic communications *alone* is insufficient to denote a "place" within the meaning of the statute. However, the statement also indicates that both a virtual space and electronic communications may be indicative of the requirement having been met where additional facts are present.

[4] The Court turns to the dictionaries considered by the Federal Circuit—The Century Dictionary further supports the Circuit's rejection of purely virtual locales from the statute. *Place*, THE CENTURY **[**8]** DICTIONARY, 4520 (Benjamin E. Smith, ed. 1911) ("7. Room to abide in; abode; lodgment; location."); *id.* ("8. Room to stand or sit in; a particular location, as a seat, or a space for sitting or standing, as in a coach, car, or public hall."); *id.* ("9. A particular locality . . . ."). Black's similarly accords. *Place*, BLACK'S LAW DICTIONARY (1st ed. 1891) ("This word is a very indefinite term. It is applied to any locality,

omitted).[6] The Federal Circuit noted that the

limited by boundaries, however large or however small. It may be used to designate a country, state, county, town, or a very small portion of a town. The extent of the locality designated by it must be determined by the connection in which it is used. 46 Vt. at 432.").

[5] The Court has surveyed additional dictionaries of the time specified, both legal and general, to ensure proper application of the statutory scope. Joseph Worchester, DICTIONARY OF THE ENGLISH LANGUAGE, 1083 (1860) (Place: "1. A particular portion of space; a locality; station; situation; position; post; site; spot."); WEBSTER'S HIGH SCHOOL DICTIONARY, 317 (1892) (Place: "Portion of space; position; locality."); Stormonth, ETYMOLOGICAL AND PRONOUNCING DICTIONARY OF THE ENGLISH LANGUAGE, 748 (7th ed. rev., 1882) (Place: "situation, site, or spot."); UNIVERSAL DICTIONARY OF THE ENGLISH LANGUAGE, 5628-29 (Hunter et al. eds., 1897) (Place (ordinary language): "2. A particular portion of space, considered as separate and distinct from the rest of space; a particular locality, spot, or site; position.") (citing *Milton: P. L.*, i. 253); Robert Gordon Latham, A DICTIONARY OF THE ENGLISH LANGUAGE (1882) (Place: "1. Particular portion of space. 2. Locality; ubiety; local relation. 3. Local existence."); J. Kendrick Kinney, A LAW DICTIONARY AND GLOSSARY, 525 (1893) (Place: "any locality limited by boundaries, whether large or small."); William C. Anderson, A DICTIONARY OF LAW, 774 (1889) (Place: "Any locality limited by boundaries, however large or small . . . . The extent of the locality is to be determined by the connection in which the word is used;" "In internal revenue acts, as applied to the place where a licensee may carry on business, construed with reference to the business . . . . In a statute forbidding betting in any 'house, office, room, or other place,' need not be covered with a roof; an umbrella is such place."); Benj. V. Abbott, DICTIONARY OF TERMS AND PHRASES, 280 (1879) (Place: "The word place has a very wide and varied signification, so that its precise meaning can only be determined by the connection in which it is used, and by having regard to the apparent purpose of the writer."); Benjamin W. Pope, LEGAL DEFINITIONS, 1179 (1920) (Place: "A 'place' is any space separated and distinguished from all other space."); BOUVIER'S LAW DICTIONARY, 2595 (1914) (Place: "The word is associated with objects which are, in their nature, fixed and territorial;" "Any piece of ground appropriated by its owner or occupier for the time being is a place within the English betting houses act but the ground must be so appropriated and must be an ascertained place.") (citations omitted); *see also* BOUVIER'S LAW DICTIONARY, 415 (1883) (Place of Business: "The place where a man usually transacts his affairs or business."); *Place of Business*, BLACK'S LAW DICTIONARY (5th ed. 1979) ("The location at which one carries on his business or employment."); Walter A. Shumaker and George Foster Longsdorf, THE CYCLOPEDIC DICTIONARY OF LAW, 694 (1901) (Place of Business: "The term implies a particular place appropriated exclusively to a local business.") (citing 38 Tex. 599).

"established" limitation "bolsters this conclusion," as it requires the business not be "transitory" and possess "sufficient permanence." Id. at 1363. "[W]hile a business can certainly move its location, it must for a meaningful time period be **[**9]** stable, established." *Id.* Fulfillment of this requirement is closely linked to the third requirement. *See* In re ZTE, 890 F.3d at 1015.

The third requirement is that "the regular and established place of business must be the place of the defendant." In re Cray, 871 F.3d at 1363. "[T]he defendant must establish or ratify the place of business." Id. at 1364. In undertaking this inquiry, the Federal Circuit provided a number of relevant considerations to assist the district courts in their analyses, including "whether the defendant owns or leases the place, or exercises other attributes of possession or control over the place," "whether the defendant conditioned employment on an employee's continued residence in the district or the storing of materials at a place in the district so that they can be distributed or sold from that place," and whether "the defendant itself holds out a place for its business." Id. However, "it must be a place *of the defendant*, not solely a place of the defendant's employee." *Id.* (emphasis added). "[A] defendant's representations that it has a place of business in the district are relevant to the inquiry." *Id.* These representations might include "whether the defendant **[**10]** lists the alleged place of business on a website, or in a telephone or other directory; or places its name on a sign associated

[6] Here, too, definitions may prove helpful in ensuring proper application of the statutory scope. *Business*, THE CENTURY DICTIONARY, 732 (1903) ("Specifically—4. Mercantile pursuits collectively; employments requiring knowledge of accounts and financial methods; the occupation of conducting trade or monetary transactions of any kind."); *Business*, BLACK'S LAW DICTIONARY (1891 ed.) (Business: "This word embraces everything about which a person can be employed. That which occupies the time, attention and labor of men for the purpose of a livelihood or profit. The doing of a single act pertaining to a particular business will not be considered engaging in or carrying on the business; yet a series of such acts would be so considered."). However, the Court considers it improper to unduly restrict its construction of the statute to permit proper venue to lie pursuant to the second half of § 1400(b) only in relation to businesses or types of business which were in existence at the time the statute was passed. No court in applying the statute, passed in 1897, would exclude from it airlines, automotive manufacturers, space transportation companies, nuclear power generators, television networks, or the various industries they support and which are supported by them.

[*941] with or on the building itself." *Id. at 1363-64*. However, such ratification alone is not enough, as "the mere fact that a defendant has advertised that it has a place of business or has even set up an office is not sufficient; the defendant must actually engage in business from that location." *Id.* The Circuit further counseled district courts to readily compare "the nature and activity of the alleged place of business of the defendant in the district" to "that of other places of business of the defendant in other venues." *Id.*

The Federal Circuit elaborated on this specific requirement recently in *In re ZTE. 890 F.3d 1008*. In determining whether an alleged place of business was *of* the defendant, the Circuit encouraged the district court to consider, on remand, "whether [the defendant] itself possesses, owns, leases, or rents the office space for the call center or owns any of the equipment located there," "whether any signage on, about, or relating to the call center associates the space as belonging to [the defendant]," and "whether the location of the call center was specified by [the defendant] **[**11]** or whether [the defendant's call center contractor] would need permission from [the defendant] to move its call center outside of the Eastern District of Texas or to stop working for [the defendant]." *Id. at 1015*.

"[A]s a matter of Federal Circuit law [], upon motion by the Defendant challenging venue in a patent case, the Plaintiff bears the burden of establishing proper venue." *Id. at 1013*.

Having summarized the law of venue as it currently exists, the Court turns now to the specific facts of this case and the application of that law thereto.

III. Discussion

As discussed above, venue lies only "in the judicial district where the defendant resides, or where the defendant has committed acts of infringement and has a regular and established place of business." *28 U.S.C. § 1400(b)*. Google argues that it meets neither requirement.

It is undisputed that when this action was filed,[7] Google was incorporated in Delaware and therefore "resided" in Delaware, not in Texas. (Dkt. No. 125 at 3 (citing Dkt. No. 1 at ¶ 2)); *see generally* Dkt. No. 141); *see also TC Heartland LLC v. Kraft Foods-Group Brand LLC, 137 S. Ct. 1514, 1521, 197 L. Ed. 2d 816 (2017)*. SEVEN does not dispute this. Accordingly, Google's residence cannot provide a basis for venue in this District.

[12]** In order for proper venue in this action to lie in this District, Google must have committed acts of infringement and have a regular and established place of business in this District. Google avers that SEVEN cannot demonstrate that it has committed acts of infringement "in this district for at least some of the asserted patents." (Dkt. No. 125 at 17). Google also avers that SEVEN cannot demonstrate that it has a regular and established place of business within this District. (*Id.* at 7).

A. Acts of Infringement[8]

[*942] "The acts of infringement referred to in the patent venue statute are those acts defined by the statute dealing with infringement." *60 Am. Jur. 2d Patents § 747*; *see, e.g., Alco Standard Corp. v. Tennessee Valley Auth., 448 F. Supp. 1175, 1182 (W.D. Tenn. 1978)* ("[T]he meaning of 'acts of infringement' in *[§] 1400(b)* must be determined by reference to *35 U.S.C. [§] 271(a)*. Accordingly, an act within the scope of [Tennessee Valley Authority Act of 1933, § 19] protection cannot be deemed an 'act of infringement' under *[§] 1400(b)*."); *Blackbird Tech LLC v. Cloudflare, Inc., No. 17-283, 2017 U.S. Dist. LEXIS 167860, at *8-9 (D. Del. Oct. 11, 2017)* ("What constitutes an act of infringement is determined by reference to the definition of patent infringement in *35 U.S.C. § 271(a)*, which states that patent infringement occurs whenever one 'without authority makes, uses or sells any patented invention within the United States during the term of the patent therefor.'"); *Roche Products v. Bolar Pharm. Co., 733 F.2d 858, 861 (Fed. Cir. 1984)*; 1 Moore's Federal Practice 0.144[9] at 1509-10 **[**13]** n.39. "[T]he 'acts of

---

[7] Venue is assessed as of the time of filing of the complaint. *See, e.g., Raytheon Co. v. Cray, 258 F. Supp. 3d 781, 787 (E.D. Tex. 2017)*, *mandamus granted on other grounds, order vacated sub nom. In re Cray, 871 F.3d 1355 (Fed. Cir. 2017)* (citing *Hoover Grp., Inc. v. Custom Metalcraft, Inc., 84 F.3d 1408, 1410 (Fed. Cir. 1996)*); *Pers. Audio, LLC v. Google, Inc., 280 F. Supp. 3d 922, 931 (E.D. Tex. 2017)*.

[8] While SEVEN brought suit against Google alleging infringement of certain claims in ten patents in this suit, Google only argues that SEVEN has failed to establish Google's commission of acts of infringement in this District as to three patents (the so-called '158, '433, and '812 Patents), leaving the other seven uncontested.

infringement' required to support venue [need not] be acts of direct infringement, and [] venue [may] lie if the defendant only induced infringement under *35 U.S.C.A. § 271(b)* or contributed to infringement under *35 U.S.C.A. § 271(c)*," and a contrarily "restricted view . . . of venue is not sound." *Gunter & Cooke, Inc. v. Southern Elec. Servs. Co., 256 F. Supp. 639, 648 (M.D.N.C. 1966)*, *aff'd*, *378 F.2d 60 (4th Cir. 1967)*; *Symbology Innovations, LLC v. Lego Sys., Inc., 158 F. Supp. 3d 916, 928 (E.D. Va. 2017)* (citing *Gunter*).[9] Where a complaint alleges infringement, the allegations "satisfy the 'acts of infringement' requirement of *§ 1400(b)*" "[a]lthough the[] allegations may be contested." *Symbology, 158 F. Supp. 3d at 928*.[10] "The issue of infringement is not **[*943]** reached on the merits in considering venue requirements." *In re Cordis Corp., 769 F.2d 733, 737 (Fed. Cir. 1985)* (citing *Gunter*).

Google first appears to argue that direct infringement of a method claim by Google alone and entirely within this District is required to meet the requirement that it has allegedly committed an act of infringement under the venue statute. (Dkt. No. 125 at 18-19).[11] It is important to note that Google does not dispute that SEVEN alleges that Google practices at least one step of the allegedly infringing method, irrespective of whether that practiced method is infringing. **[**14]** (*See generally id.*) However, Google argues that "SEVEN has failed to plead that Google performs each step of the method claim in this District, which is required to show that Google has committed an act of infringement in this District." (*Id.* at 18). Google relies on *NTP, Inc. v. Research in Motion, Ltd*. for this proposition. *418 F.3d 1282, 1317-18 (Fed. Cir. 2005)* (ruling that "[i]t is well established that a patent for a method or process is not infringed unless all steps or stages of the claimed process are utilized" and that a process "cannot be used within" a place "unless each of the steps is performed within" that place).

However, this exact argument has been previously rejected by the courts. "Contrary to Plaintiff's argument, not *all* of the alleged infringing activity needs to have occurred within [the District] so long as some act of infringement took place there." *Blackbird Tech, 2017 U.S. Dist. LEXIS 167860, at *10* (specifically rejecting the Plaintiff's proposition (opposing a *§ 1404(a)* motion) that while "some portion of the accused system is located in the Northern District of California, the data channels connecting the various network elements are found throughout the country," preventing "California

---

[9] Nor do the alleged acts of infringement need be substantial or numerous. A single alleged act of infringement may be sufficient to properly establish venue. *Rackman v. Texas Instruments, Inc., 712 F. Supp. 448, 450 (S.D.N.Y. 1989)* (finding "no support for [the] contention that *28 U.S.C. § 1400(b)* requires more than 'de minimis' infringement").

[10] *Accord* *Plexxikon Inc. v. Novartis Pharms. Corp., No. 17-cv-04405-HSG, 2017 U.S. Dist. LEXIS 201984, at *3 (N.D. Cal. Dec. 7, 2017)* (citing *Cordis*); *RegenLab USA LLC v. Estar Techs. Ltd., No. 16-cv-08771 (ALC), 2017 U.S. Dist. LEXIS 131627, at *6 n.2 (S.D.N.Y. Aug. 17, 2017)* ("[Defendants] assert in passing that they have not committed acts of infringement in the Southern District of New York, a requirement under the second prong of *§ 1400(b)*. With respect to infringement, at this stage, it suffices that [Plaintiff] alleges that each defendant made sales in New York of the product at issue.") (citing *Cordis*); *Ballard Med. Prods. v. Concord Labs., Inc., 700 F. Supp. 796, 799 (D. Del. 1988)* ("The allegation of manufacture of the prototype meets defendants' burden as to venue since courts have consistently held an allegation of infringement is itself sufficient to establish venue and the moving party is not required to demonstrate actual infringement by defendant's device.") (citing *Cordis and Funnelcap, Inc. v. Orion Indust. Inc., 392 F.Supp. 938, 941 (D.Del.1975)*; *CAO Lighting, Inc. v. Light Efficient Design, No. 4:16-cv-00482-DCN, 2017 U.S. Dist. LEXIS 170052, at *5 (D. Idaho Oct. 11, 2017)* ("The parties do not dispute that CAO has alleged that Light Efficient Design has committed acts of infringement in Idaho. Therefore, the Court need only address whether Light Efficient Design has a regular and established place of business in Idaho."); *see also* 17 *Moore's Federal Practice - Civil § 110.39* (2018) ("In [the] context of [post-*TC Heartland* *§ 1400(b)* analysis], the requirement that the defendant commit an act of infringement in the proposed forum is not particularly troublesome. The patent statute defines acts of infringement to include making, using, or selling patented inventions without authority, or importing, selling, or using products made by patented process. This definition encompasses indirect as well as direct infringement. Traditionally, courts have required only an adequate allegation of infringement under the statute to assert venue.").

[11] (*Id.* ("On its face, the Complaint is deficient because SEVEN only specifically identifies a single step purportedly performed by Google in this District for each of the asserted method claims for the '158, '433, and '812 Patents.")).

[from being] the situs of infringement.").[12] As noted above, the acts of **[**15]** infringement required to support venue in a patent infringement action need not be acts of direct infringement, and venue does lie if the defendant only induced the infringement or *contributed* to the infringement in the forum. *See* Gunter, 256 F. Supp. at 648; *see also* Dover Corp. v. Fisher Governor Co., 221 F. Supp. 716, 720 (S.D. Tex. 1963) ("I do not accept the defendant's theory of patent venue that 'acts of infringement' for venue purposes are exclusively defined as direct making, using or selling. The defendant's theory would virtually eliminate the availability of venue alternatives to a plaintiff suing a corporate 'contributory infringer,' for the suit would have to be brought at the place of the defendant's incorporation. I can discern neither the logic nor fairness of such a theory, for the place of incorporation of a 'contributory infringer' may be far removed from its principal place of business and from the place of occurrence of the acts or wrongs for which liability is imposed.").[13]

[*944] The facts here comport with those of *Blackbird*. 2017 U.S. Dist. LEXIS 167860. The court in *Blackbird* "*reject[ed] the contention that acts of infringement were not done in California because the entire method allegedly was not practiced in the forum*, the court noting that 'not all of the alleged infringing **[**16]** activity needs to have occurred within California so long as some act of infringement took place there,' and as the complaint alleged both method and apparatus claims, and . . . finding that the accused infringers 'make or use the accused functionality' in the forum, and this was sufficient to show that § 1400(b) venue was proper in the transferee forum." 5 Annotated Patent Digest § 36:153.80 (discussing Blackbird Tech, 2017 U.S. Dist. LEXIS 167860) (emphasis added).[14] Google does not appear to dispute that SEVEN "explicitly alleged that at least one step of each of the claims is performed in this District." (Dkt. No. 141 at 27).[15] This is **[*945]** sufficient

---

[12] *See also* Grant St. Grp., Inc. v. D&T Ventures, LLC, No. 10-1095, 2012 U.S. Dist. LEXIS 505, at *15 n.5 (W.D. Pa. Jan. 4, 2012) (rejecting an application of *NTP* in "a personal jurisdiction analysis," and noting that "[*NTP*] speaks to the merits of the infringement claim").

[13] As SEVEN notes, "[t]he Federal Circuit did not hold, and has never held, that when a defendant carries out the steps of a method claim in multiple districts, there can be no act of infringement in any of them . . . . Such a ruling would be nonsensical, as it would mean that an act of infringement could occur within the United States without taking place in any district in the United States." (Dkt. No. 141 at 28). Google responds to this argument by noting that this result "does not eviscerate the venue statute as venue would still be proper in the district where the defendant resides," (Dkt. No. 148 at 9), and confirmed this position at argument. (Dkt. No. 193 at 26:24-27:7 ("THE COURT: So with a method claim, as long as an infringer made sure that all the steps weren't practiced in the same district, they could never properly be sued anywhere? [] Is that the -- is that the logical extension of your argument? MR. VERHOEVEN: That is an issue that would need to be dealt with."), 28:1-9 ([MR. VERHOEVEN:] "I would say that even if you had a method claim where each of the steps was in a different venue, you can still sue somebody in the state of incorporation. So there's two prong -- there's two ways that you can get venue, and -- and so -- THE COURT: So instead of there never being a place where you could get venue, you would be limited only to the state of incorporation. MR. VERHOEVEN: Yes. Yes, Your Honor."). However, the result required by Google's reading of the statute undoubtedly forecloses the ability of a plaintiff to avail itself of half of the special patent venue statute. This would do violence to the statutory venue grant. That is the world § 1400(b) was intended to leave behind. Indeed in its authoritative discussion on the underlying purpose and policy of § 1400(b) in *In re Cray*, the Federal Circuit noted that the requirement of some courts (equivalent to the position Google urges here) which made it "necessary to sue a defendant in its place of incorporation, and 'the corporations thus have an opportunity to infringe upon patents and almost escape any responsibility for it by reason of the difficulty of finding them in order to sue them, for it is very inconvenient to travel across the continent to sue them when they are infringing in a business established near the plaintiff or owner of a patent,'" was abrogated by § 1400(b), which, "of course[,] allows broader venue than merely the place of a defendant's incorporation." 871 F.3d at 1361 (citing 29 Cong. Rec. 2719 (1897) (statement of Sen. Platt) and Brunette Mach. Works, Ltd. v. Kockum Indus., Inc., 406 U.S. 706, 713 n.13, 92 S. Ct. 1936, 32 L. Ed. 2d 428 (1972)). Accordingly, Google's supposed preservation of the venue statute leaves little of the "broader" § 1400(b) provision standing and must be rejected.

[14] The *Blackbird* court also accepted the Defendants' representation that the allegedly infringing apparatus was "made" in the proposed forum.

[15] (*See* Dkt. No. 34 at ¶¶ 47 ("Google infringes at least claim 10 of the '158 Patent under at least ***35 U.S.C. § 271(a)***. Google, for example, practices every step of at least claim 10 in the United States, including steps that it practices in this District."), 79 ("Google infringes at least claims 1 and 16 of the '433 Patent under at least ***35 U.S.C. § 271(a)*** and ***(b)***. Google makes, uses, sells, offers to sell, or imports into the United States the Google Play store which meets every limitation of at least claim 1. Further, Google, for example, practices every step of claim 16 in the United States, including steps that it practices in this District."), 86 ("Google infringes at least claims

to establish that acts of infringement were committed within this District for venue purposes under the patent venue statute.

Google also argues that merely alleging acts of infringement occurred in the District is insufficient under § 1400(b). Under Google's view, "the acts of infringement alleged in SEVEN's Complaint [must be] *tied to or related to* Google's purported regular and established place of business in this District," as "required" by 28 U.S.C. § 1400(b). (Dkt. No. 125 at 19) (emphasis added). The Court disagrees.

As this Court explained in Part II, courts applying the venue statute must hew closely to it. This **[**17]** duty constrains courts, forbidding minimizing or reading out requirements laid out by the statute; it similarly constrains courts from inserting or inventing requirements not present within the statute. Bates v. United States, 522 U.S. 23, 29, 118 S. Ct. 285, 139 L. Ed. 2d 215 (1997) ("[W]e ordinarily resist reading words or elements into a statute that do not appear on its face."). As *Raytheon Co. v. Cray, Inc.* noted, the Federal Circuit has never addressed the question of whether the acts of infringement required by § 1400(b) must be related to the regular and established place of business of the defendant. 258 F. Supp. 3d at 791-92. Google argues, however, that the language of § 1400(b), while written as setting proper venue in a judicial district "where the defendant has committed acts of infringement and has a regular and established place of business," actually only sets proper venue in a judicial district "where the defendant has committed acts of infringement *at their* regular and established place of business." The clear substitution of statutory language which Google's proposition requires demonstrates that it is incorrect. Additionally, the venue statute is "designed to protect the defendant against the risk that a plaintiff will select an unfair or inconvenient place of trial." Utterback v. Trustmark Nat'l Bank, 716 Fed. Appx. 241, 244 (5th Cir. 2017), *cert. denied* ***[**18]*** , *138 S. Ct. 1699, 200 L. Ed. 2d 954 (2018)*. It is not "unfair" to require a defendant to answer suit in a district wherein a defendant has a regular and established place of business *and* is alleged to have committed acts of infringement. Google would have the Court improperly read a requirement into the statute where none exists and ignore the facial independence of the statutory elements. The Court declines to do so.

While some courts have previously held that there must be some "reasonable or significant relationship between the accused item and any regular and established place of business of the accused in the judicial district," Scaramucci v. FMC Corp., 258 F. Supp. 598, 602 (W.D. Okla. 1966),[16] many other courts reached the opposite conclusion, holding that "the regular and established place of business need not be the business connected with the alleged patent infringement." Ferguson v. Ford Motor Co., 77 F. Supp. 425, 436 (S.D.N.Y. 1948). As one court explained:

> Nothing in the language of Section 1400(b) justifies the conclusion that a defendant's place of business in the district must have some connection with the accused device. The statute requires only that the defendant have committed acts of infringement in the district and have a regular and established place of business there; there is no requirement that the two factors be related.

Am. Can Co. v. Crown Cork & Seal Co., 433 F. Supp. 333, 336 (E.D. Wis. 1977) (quoting Bourns, Inc. v. Allen-Bradley Co., 173 U.S.P.Q. 567, 568 (N.D. Ill. 1971)); *see also* ***[**19]*** Chadeloid Chem. Co. v. Chicago Wood Finishing Co., 180 F. 770, 771 ***[*946]*** (C.C.S.D.N.Y. 1910) (Hand, J.) ("Even if they committed no act of infringement there, it would still be a place of business within the act, which clearly differentiates between the two."). The conjoined reading which Google advances improperly introduces a new requirement into the statutory text. Tesoro Hawaii Corp. v. United States, 405 F.3d 1339, 1347 (Fed. Cir. 2005) ("[I]t is the duty of the courts to enforce [the statute] according to its obvious terms and not to insert words and phrases so as to incorporate therein a new and distinct provision.") (citing Gibson v. United States, 194 U.S. 182, 192, 24 S. Ct. 613, 48 L. Ed. 926, 39 Ct. Cl. 551 (1904) ("Had Congress intended that such allowances as theretofore given should be continued, or to reserve, the right to commutation as to the sea ration, it would have been very easy to have inserted apt words which would have rendered effectual this purpose. But the terms of the law undertaking to revise former laws upon the subject make no such reservation as is contended for, and we

---

1 and 10 of the '812 Patent under at least ***35 U.S.C. § 271(a)*** and ***(b)***. Google, for example, practices every step of at least claim 1 in the United States, including steps that it practices in this District. Further, Google makes, uses, sells, offers to sell, or imports into the United States servers that meet every limitation of at least claim 10.")).

[16] *See also* Jeffrey Galion, Inc. v. Joy Mfg. Co., 323 F. Supp. 261, 266-67 (N.D. W. Va. 1971).

think we are not at liberty to add to the statute by inserting it."), and *United States v. Temple, 105 U.S. 97, 98, 26 L. Ed. 967, 17 Ct. Cl. 436 (1881)* ("Our duty is to read the statute according to the natural and obvious import of the language, without resorting to subtle and forced construction for the purpose of either limiting or extending its operation. When the language is plain, we have no right to insert words **[**20]** and phrases, so as to incorporate in the statute a new and distinct provision.") (citations omitted)).

While not controlling, the Fifth Circuit addressed this issue in *Gaddis v. Calgon Corp., 449 F.2d 1318 (5th Cir. 1971)*, concluding that it was error to "requir[e] a showing that the particular division [of the business] charged with the infringements [*sic*] had a regular and established place of business present in the District." *449 F.2d at 1320* (emphasis omitted). The Fifth Circuit instead held that the totality of the circumstances together "add[ed] up to enough to establish venue," and rejected the same connection that Google now advances. *Id. at 1320*.[17]

This Court therefore rejects Google's proposition that the special patent venue statute requires that alleged acts of infringement by the Defendant pled to meet the requirements of *§ 1400(b)* must be "tied to or related to" the regular and established place of business of the Defendant, which is separately required by *§ 1400(b)*. The Court finds that SEVEN has adequately pled acts of infringement within this District as to the claims related to the three objected-to patents-in-suit sufficient to meet the requirements of *28 U.S.C. § 1400(b)*.[18]

[*947] B. Regular and Established Place of Business

This Court now turns to the issue of **[**21]** whether Google has a regular and established place of business within this District within the meaning of the patent venue statute, *28 U.S.C. § 1400(b)*. The Court believes adherence to the statutory requirements, informed by Federal Circuit guidance, is best demonstrated by addressing each of the requirements identified in *In re Cray* individually. *871 F.3d 1355*. Proper venue lies in districts where each requirement of the venue statute is met. Only where one of the statutory requirements identified by the Circuit is not met is venue to be found improper.

i. Background[19]

---

[17] This view is repeated by commentators and case law alike. *60 Am. Jur. 2d Patents § 747* ("The regular and established place of business does not need to be a business connected with the alleged infringement."); *Cabot Corp. v. WGM Safety Corp., 562 F. Supp. 891, 892 (D. Mass. 1983)* ("I do not read *§ 1400(b)* as requiring that there be some connection between the acts of infringement alleged and the regular and established place of business within this district."); *see also supra*, at 8

[18] The Court notes that, to the extent Google objects to the inclusion of system claims of the objected-to patents in the acts of infringement analysis, the Court declines to address that issue at this time. (*See* Dkt. No. 125 at 25 ("SEVEN also asserts a system claim of the '433 Patent (claim 1), which recites "a first server" and "a second server." While SEVEN alleges "[c]ertain Google Play servers" may perform the recited functionality, it does not allege that any of these servers are in this District, that the servers or the accused functionality was made, designed, or developed in this District, or that Google has committed acts of infringement in this District.") (citations omitted). First, Google makes no effort to define the full scope of the system at issue in the '433 Patent, even though the system specifically includes mobile devices. *See* U.S. Pat. No. 9,386,433 at 20:2-5 ("1. A system for providing mobile network services comprising: a first server communicatively coupled to a mobile device over a mobile network . . ."). It may well be that one part of the system (the Google Play servers) is not present in this District; this argument says nothing about other clearly identified parts of the system specifically alleged to be present and infringing by SEVEN. (Dkt. No. 34 at ¶ 81 ("When using the Google Play app, one or more of these servers are communicatively coupled to a user's mobile device over a mobile network such as 3G, LTE, or WiFi."); *id.* at ¶ 82 (identifying "end users in this District"). And it cannot be disputed that the system's various parts must all be considered in any analysis of infringement. *See Intellectual Ventures I LLC v. Motorola Mobility LLC, 870 F.3d 1320, 1328 (Fed. Cir. 2017)* (requiring "the patentee to demonstrate that the direct infringer obtained 'benefit' from each and every element of the claimed system"). Accordingly, the Court may properly hold that some alleged infringement of the system claim has occurred within this District and may find that partial alleged infringement sufficient to meet the acts of infringement requirement as to the system claim. *Blackbird Tech, 2017 U.S. Dist. LEXIS 167860*. Second, to the extent that this is insufficient to establish acts of infringement under *§ 1400(b)* as to the system claim of the '433 patent, the Court holds that it may exercise pendent venue over any claims of a single patent where the Court has found proper venue as to at least one claim of that patent.

[19] (Dkt. No. 141 at 2-8 (cleaned up)). This general background section is directly quoted from SEVEN's briefing. This is necessary to provide the factual framework within which the

Google is in the business of delivering information, including digital content such as movies, music, apps, and advertising. Google is a multinational technology company in the business of storing, organizing, and distributing data. More precisely, "Google is an information company." Its vision is "to provide access to the world's information in one click," and its mission is "to organize the world's information and make it universally accessible and useful." Making information available to people wherever they are and as quickly as possible is critical to Google's business. As Google's CEO, Sundar Pichai, explains, "We want to make sure that no matter **[**22]** who you are or where you are or how advanced the device you are using—Google works for you." To meet this goal, Google developed a content-delivery network that it calls the Edge Network.

Google delivers information through its Edge Network. Google provides web-based services, such as YouTube and Google Play, to users throughout the **[*948]** world. These services are in high demand. Google reports that Google Play reaches more than 1 billion Android users and that YouTube serves over 1.5 billion users per month. Studies show that YouTube alone is responsible for approximately 20% of all internet traffic. Delivering that much data requires lots of bandwidth, and when the data is being transmitted to large numbers of geographically diverse users it must traverse multiple network paths at different times. It also costs money. The larger the data and the farther it has to travel, the greater the cost.

Google addresses these challenges with its Edge Network, which has three elements: Core Data Centers, Edge Points of Presence, and Edge Nodes. The Core Data Centers (there are eight in the United States) are used for computation and backend storage. Edge Points of Presence are the middle tier of the **[**23]** Edge Network and connect the Data Centers to the internet. Edge Nodes are the layer of the network closest to users. Popular content, including YouTube videos, video advertising, music, mobile apps, and other digital content from the Google Play store, is cached on the Edge Nodes, which Google refers to as Google Global Cache (GGC).

Google Global Cache is recognized as "one of Google's most important pieces of infrastructure," and Google uses it to conduct the business of providing access to the world's information. GGC servers in the Edge Nodes function as local data warehouses, much like a shoe manufacturer might have warehouses around the country.[20] Instead of requiring people to obtain information from distant Core Data Centers, which would introduce delay, Google stores information in the local GGC servers to provide quick access to the data.

"Caching and localization are vital for [Google's] optimization of network resources." Because "hosting all content everywhere is inefficient, it makes sense to cache popular content and serve it locally." Doing so brings delivery costs down for Google, network operators, and internet service providers. Storing content locally also allows it **[**24]** to be delivered more quickly, which improves user experience: "Serving content from the edge of the network closer to the user improves performance [and] user happiness." To achieve these benefits, Google has placed Edge Nodes throughout the United States, including in this District. Google describes these nodes as the "workhorse[s] of video delivery."

Just like brick-and-mortar stores, Google's GGC servers independently determine what content to cache based on local requests.[21] The GGC servers in Google's Edge Nodes include software that Google refers to as "Ustreamer (actually µstreamer, i.e. micro-streamer)." Ustreamer is "responsible for

---

Court operates in this analysis and its direct quotation from the Plaintiff's briefing is largely a function of Google not providing any general overview of its business operations and how its Edge Network functions/supports its core business functionalities. While it is in Google's interests to minimize how its Edge Network and Google Global Cache ("GCC") servers operate within, support, and benefit its various business functionalities in order to support its contentions that it does not "do business" through its Edge Network and GCC servers, SEVEN's statements are, generally, not contradicted or otherwise undermined by Google in either its Motion or Reply. This section is intended to 'set the stage' for the specific fact-intensive analysis the Court must undertake in its application of the statute to the case at bar.

[20] Google disputes this characterization. (Dkt. No. 148 at 3 ("GGC servers are not warehouses.")). This is a principal objection and will be addressed *infra*.

[21] Google disputes this characterization. (*See* Dkt. No. 148 at 1 ("There is no 'regular and established place of business'")).

serving video content from YouTube and other Google services, along with other large content such as Google Play applications and Chrome downloads." It operates on a content-delivery platform "at the edge of Google's network" called "bandaid"; it "does not run in the core (except for some internal testing purposes), unlike the majority of the Google services, such as search or gmail."

Using ustreamer and bandaid, a GGC server "handles requests directly from its clients, predominantly YouTube's video **[*949]** players." When such a request is received, if the **[**25]** content is stored in the node's local cache, "the node will serve [it] . . . to the end user, improving the user experience and saving bandwidth." If cache-eligible content is not already stored on the node, and the content is cache-eligible, "the node will retrieve it from Google, serve it to the user, and store it for future requests."

Ustreamer is largely "autonomous," "in the sense that almost all decisions related to serving a particular request are made locally, without coordinating with other servers." Like a brick-and-mortar store sells directly to customers from inventory and stocks that inventory based on local customer demand, ustreamer in each GGC node decides—independently from other nodes in Google's Edge Network—whether to serve requested content, whether to cache content, and whether to send requests to other servers.[22]

Google's GGC servers are housed in spaces in the District leased by Google.[23] Google's GGC servers are housed in spaces leased[24] by Google from Internet Service Providers (ISPs) whose networks "have substantial traffic to Google and are interested in saving [bandwidth]." Hosting Google servers allows ISPs to save both bandwidth and costs, as they "do not incur **[**26]** the expense of carrying . . . traffic across their peering and/or transit links."

When an ISP agrees to host a GGC server, the parties enter into a Global Cache Service Agreement, under which Google provides hardware and software—including GGC servers and software—to be housed in the host's facilities; technical support; service management of the hardware and software; and content distribution services, including content caching and video streaming. In exchange, the host provides, among other things, a physical building, rack space where Google's computer hardware is mounted, power, and network interfaces. "All ownership rights, title, and intellectual property rights in and to the Equipment [i.e., the hardware and software provided by Google] . . . remain in Google and/or its licensors."

Google GGC servers located in this District cache Google's products and deliver them to residents of this District. Google does not dispute the following.

1. Multiple ISPs hosted GGC servers in the Eastern District of Texas for at least the five months leading up to the filing of the lawsuit (and they continue to do so).

2. Suddenlink Communications, for example, is an ISP that hosts six GGC servers in **[**27]** Tyler, Texas.

3. CableOne is an ISP that hosts three GGC servers in Sherman, Texas, and three GGC servers Texarkana, Texas.

[*950] 4. Google caches content on its GGC servers located in the Eastern District of Texas.

5. Google's GGC servers located in the Eastern District of Texas cache content that includes, among other things: (i) video advertising; (ii) apps; and (iii) digital content from the Google Play store.

6. Google's GGC servers located in the Eastern District of Texas deliver cached content referenced in number 5, above, to users in the Eastern District of Texas.

7. Google generates revenue (i) by delivering video advertising, (ii) from apps, and (iii) from digital content in the Google Play store.

8. Google treats its GGC servers in the Eastern District of Texas the same as it treats all of its other GGC servers in the United States.

---

[22] Google disputes this characterization. (*See* Dkt. No. 148 at 1 ("There is no 'regular and established place of business'")).

[23] Google disputes that it leases anything. (Dkt. No. 148 at 5 ("Google does not own, lease, or otherwise exercise possession or control over the ISPs' buildings or rooms housing the GGC servers in this District")). This is a principal objection and will be addressed *infra*.

[24] Google disputes that it leases anything. (Dkt. No. 148 at 5 ("Google does not own, lease, or otherwise exercise possession or control over the ISPs' buildings or rooms housing the GGC servers in this District")). This is a principal objection and will be addressed *infra*.

The photographs below show Google's GGC servers hosted by Suddenlink and the building where they are located at 322 North Glenwood Boulevard, Tyler, Texas 75702.

ii. Physical Place

Google argues that "GGC servers are not 'physical places of business.'" (Dkt. No. 125 at 9). "A server is a piece of hardware or equipment, not a place. SEVEN **[**28]** itself has described the servers as 'physical objects housed at physical locations' (Dkt. [No.] 76 at 14), which is exactly right. The servers are objects; the locations where they are stored are the places." (*Id.*) "Contrary to SEVEN's allegation that 'a physical, geographical location' can be broader than a building or quarter (Opp. 12), all three 'locations' identified in *Cray* were buildings or quarters: employees' home offices, distribution centers, and a building occupied by the secretarial service." (Dkt. No. 148 at 2). "Even people (employees) are physical objects that enclose space, which alone cannot establish venue. SEVEN's definition directly contradicts *Section 1400(b)* and *Cray*, both of which require a 'place' to establish venue, not objects or physical things." (*Id.*)

Google relies on a sister court's ruling from this District considering these GGC servers to support its contention. "The GGC servers are not 'places' under the meaning of the statute and therefore cannot establish a regular and established place of business in this [D]istrict." *Personal Audio, LLC v. Google, Inc., 280 F. Supp. 3d 922, 2017 WL 5988868, at *10 (E.D. Tex. 2017)*.

With respect to its sister court, this Court disagrees with that conclusion. A revisiting of **[**29]** the ultimate decision of *Personal Audio* on this issue is not only possible but compelled by the facts of this case. Additionally, in this Court's opinion, neither the statute nor the Federal Circuit's guidance in *In re Cray* permit the result reached by that court.[25]

[25] Other courts examining similar facts have reached the same conclusion as this Court now reaches. *Peerless Network, Inc. v. Blitz Telecom Consulting, LLC, No. 17-CV-1725 (JPO), 2018 U.S. Dist. LEXIS 49628, 2018 WL 1478047, at *3 (S.D.N.Y. Mar. 26, 2018)* (holding that "a shelf containing a piece of Local Access's telecommunications equipment" "is a 'physical place in the district' insofar as it is '[a] building or a part of a building set apart for any purpose.'") (citing *In re Cray, 871 F.3d at 1362*).

Specifically, the Court recalls the conclusion it noted *supra* n.3. *Section 1400(b) of Title 28, United States Code* **[*951]** lays proper venue where "the defendant . . . has a regular and established place of business." As the Federal Circuit instructed in *In re Cray*, "[t]he statute [] cannot be read to refer *merely* to a virtual space or to electronic communications from one person to another." *871 F.3d at 1362* (emphasis added). Any reading of the statute which "authorizes" such places must be rejected. *Id.* However, the Federal Circuit's inclusion of "merely" indicates that while a virtual space or electronic communications *alone* are insufficient to denote a "place" within the meaning of the statute, they may, with more, be indicative of the requirement having been met. This is precisely the situation here.

Of course, it would run counter to the statutory requirements to find proper venue in a district where there was *no* physical presence of a given defendant. A defendant who does not establish **[**30]** or permit a physical presence within a district *of its own volition* may not be brought into a district pursuant to the venue statute by the acts of another. To hold otherwise contravenes the language of the statute, requiring the defendant to "[have] a regular and established place of business" within the district. *28 U.S.C. § 1400(b)*.[26] This is true even where there may be citizens of that district who, at *their* places (homes, for example) connect to that defendant's website and engage that defendant in business or where a defendant's employees have *their own* places in which they perform their employment. *In re Cray, 871 F.3d at 1363* ("[I]t must be a place of the defendant, not solely a place of the defendant's employee.") (emphasis omitted).

Here, however, there is more than "merely" "a virtual

[26] Accordingly, the concern expressed in *Personal Audio* that "[m]aybe even every handheld device sold by Verizon would become a place of business for Verizon because the end-user signed an agreement with Verizon regarding Verizon's exclusive control of the device," is clearly seen to be too far afield from the statutory text. *280 F. Supp. 3d at 934*. Such a holding could not be supported by proper application of the law; proper reading of the statute, guided by *In re Cray*. Such would adequately prevent the "distort[ion] of the statute" feared by the *Personal Audio* court. *Id.*

space or [] electronic communications from one person to another." *Id. at 1362*. The "place" is specifically localized: a physical server occupying a physical space. Not only does Google exercise exclusive control exercised over *the digital aspects of the GGC*,[27] Google exercises exclusive control over the *physical server and the physical space within which the server is located and maintained*.

In this regard, the Court has considered the Beta Service Agreement: Google Global Cache (GGC) Service between Google and Suddenlink ("the Suddenlink Agreement") (Dkt. No. 141-23).[28] It reveals that Google exacts far more control than may **[*952]** be suspected from a general lease arrangement. Google *requires* ISPs such as Suddenlink to provide "[r]ack space, power, network interfaces, and IP addresses, as specified in the following table [omitted], in consultation with Google";[29] "[r]emote assistance and installation services described in SCHEDULE 'A'"; "[n]etwork access between the Equipment and Host network subscribers"; and "[r]emote high bandwidth access, sufficient for Google to download upgrade images of GGC to the Equipment, unless separate arrangements are agreed with Google." (Dkt. No. 141-23 at 1). The Suddenlink Agreement makes it clear that the ISP *does not own* the server(s); *Google owns the servers*. (Dkt. No. 141-23 at 2 (In the event of termination of the Agreement: "Host will *remove, package and ship* (shipping charges will be pre-paid directly by Google to the carrier, and Host will undertake such **[**32]** removal and packaging to be undertaken in a commercially reasonable manner) all Equipment back to Google within fifteen (15) calendar days of effective date of termination. If Host fails to do so, *Google will have the right to: (a) charge Host and Host will pay the fair market value of the Equipment; or (b) recover and take possession of such Equipment*, and for this purpose may enter any premises of Host where such equipment is located during normal working hours to remove Equipment. Host will promptly surrender the Equipment to Google in as good order and condition as originally delivered, reasonable wear and tear excepted.") (emphasis added)). Google is not even required to replace faulty servers under the Suddenlink Agreement. (Dkt. No. 141-23 at 7 ("Google Services: Google will provide the following services in beta: . . . 3. replace faulty Equipment (at Google's cost and sole discretion)")). This Agreement is not a mere lease of digital space or computing power; it is the installation of Google's own servers in a physical space *that becomes Google's*. Following installation of the GGC server, the ISP is required to provide Google explicit details regarding Google's server's installation **[**33]** location. (*Id.* at 3 ("Contact & Location Details: As soon as practicable after the Effective Date, the parties will advise each other in writing (which may be sent electronically) of the following: . . . (c) Equipment location (address/floor/rack)")). Once installed, it is considered a permanent fixture. There is no dispute that the Suddenlink Agreement requires that, in order for an ISP to move a previously installed GGC from one location to a new location, it must secure Google's permission, *which Google may not permit "at its sole discretion."* (Dkt. No. 141-23 at 2 ("Change Notification: *Host will provide Google no less than thirty (30) days' written notice of any proposed relocation of the Equipment or change of IP address*. Host may propose relocation at any time. *Google, at its sole discretion, may elect not to accept the proposed relocation* but will reasonably consider any such relocation and discuss all reasonable options with Host.") (emphasis added)). Google's ownership of the server and its contents is absolute, as is Google's control over the server's location once it is installed. (Dkt. No. 141-24 at 2 ("Restriction on Use of Equipment: *All ownership rights, **[*953]** title, and intellectual **[**34]** property rights in and to the Equipment shall remain in Google and/or its licensors*. THE EQUIPMENT OR ANY PORTION THEREOF MAY NOT BE USED, COPIED, TRANSFERRED, REVERSE-ENGINEERED, OR MODIFIED EXCEPT AS EXPRESSLY PERMITTED BY

---

[27] Which may well constitute "merely" a "virtual space" without more and, thus, not meet the statutory requirement. For example, while an Amazon Web Services data center may be located in a particular district, an online business which utilizes Amazon's cloud web hosting solution *on the terms offered **[**31]** by Amazon and without any physical equipment of its own present within the data center* would, undoubtedly, not be subject to proper venue under *§ 1400(b)* in that district.

[28] The Suddenlink Agreement is only one instance of GGC agreements existing between Google and ISPs within the Eastern District of Texas. The Court discusses it as an exemplar. Such GGC agreements also include Google's agreement with CableOne, an ISP that hosts three GGC servers in Sherman, Texas, and three GGC servers Texarkana, Texas. (Dkt. No. 141 at 19 ("Google GGC servers have been operating (i) in Tyler under the Global Cache Agreement with Suddenlink since at least December 2015 and (ii) in Sherman and Texarkana under the agreement with CableOne since at least August 2015") (citations omitted)).

[29] (*See* Dkt. No. 141-23 at 6 ("Space: The Host shall provide Google rack space for the Equipment located at the Space within Host premises.")).

THIS AGREEMENT. Host must not, without the prior written consent of Google (which may be withheld in its sole discretion), access, use, or dispose of the Equipment, in whole or in part.") (emphasis added)).

This is not a partnership, wherein an ISP may independently act on Google's behalf in administering the GGC. To the contrary, the Suddenlink Agreement expressly disclaims any such relationship. (Dkt. No. 141-24 at 2 ("No Partnership, No Exclusivity: The parties are independent contractors, and this Agreement does not create an agency, partnership or joint venture. This Agreement is not intended to, nor does it create, any agency, partnership, joint venture or other profit-sharing arrangement, nor does it create an exclusive relationship between the parties. This Agreement places no restrictions of any type on either party's ability to freely compete or to enter into agreements with other entities or individuals.")). Indeed, Google's total control over the **[**35]** GGC server's physical presence within the ISP may be best illustrated by the Suddenlink Agreement's requirement that tasks such as the "physical switching of a toggle switch;" "power cycling equipment (turning power on and/or off);" and "*tightening screws*, cable ties, or securing cabling to mechanical connections, plug;" may be performed "only with specific and direct step-by-step instructions from Google." (Dkt. No. 141-23 at 6) (emphasis added).

This level of control in the physical world exemplifies how the physical presence of the GGC server within this District constitutes more than "merely" "a virtual space or [] electronic communications from one person to another." *In re Cray, 871 F.3d at 1362*. Indeed, such control in the physical realm over a specific physical space establishes that, irrespective of the determinations related to the other *§ 1400(b)* requirements, there is a physical place which this Court may examine to determine if it is a regular and established place of business and whether it is a place of the defendant.[30]

[*954] Accordingly, the Court finds that, in this case, the GGC server itself and the place of the GGC server, both independently and together, meet the statutory requirement of a "physical **[**36]** place."[31] SEVEN has met its burden to demonstrate satisfaction of this statutory requirement.

iii. Regular and Established Place of Business

Google argues that "[e]ven if the GGC servers were 'places' . . . SEVEN fails to provide a basis to conclude that these servers are 'places of businesses,' let alone regular and established places of business of Google." (Dkt. No. 125 at 10). The Court will address the "of Google" argument in Part III.B.iv., *infra*, but as to whether the GGC servers and the place where the servers are lawfully housed are "places of business" within the meaning of the statute, the Court reaches the opposite conclusion—they undoubtedly are.

---

[30] This conclusion is buttressed by statements made by Google at argument on the instant Motion. Google agrees that "all virtual space has to have [associated] hardware." (Dkt. No. 193, Hr'g Tr. (sealed) at 15:2). Google admits that it owns the server. (*Id.*, Hr'g Tr. (sealed) at 7:14-16 ("THE COURT: Would you agree that Google owns the server? MR. VERHOEVEN: Yes.")). Google agrees that Google possesses a "right" for its server to be "placed" in and occupy the ISP's "physical location" by means of the Suddenlink agreement and that without the agreement "its server would be trespassing on someone else's property." (*Id.*, Hr'g Tr. (sealed) at 7:17-8:4 ("THE COURT: And would you agree that Google acquires the right for its server to be placed in the ISP's physical location by means of this agreement? MR. VERHOEVEN: Yes. Yes, Your Honor. THE COURT: And without the agreement, Google's property, its server, would be trespassing on someone else's property, correct? MR. VERHOEVEN: I mean, that's a hypothetical, Your Honor. THE COURT: Well, there would be no right to be there outside of this agreement? MR. VERHOEVEN: As a general principle, yes, you never have a right to invade somebody else's prop - real estate property . . . ")). There is no other basis for permitting the GGC server to reside within the ISP separate and apart from the Suddenlink Agreement. (*Id.*, Hr'g Tr. (sealed) at 8:17-21 ("THE COURT: You're not pointing to any other document or any other basis outside of this, as you call it, hosting agreement to support Google's right to have its property housed at these locations, correct? MR. VERHOEVEN: I guess I'm not, Your Honor.")). The ISPs are "not allowed to open the server. You're not allowed to manipulate the server. You're not allowed to unscrew the form factor and take it apart." (*Id.*, Hr'g Tr. (sealed) at 10:14-17 (MR. VERHOEVEN)).

[31] The Court notes that this conclusion is able to be reached largely due to the venue discovery Ordered by the Court in this case. (Dkt. No. 107). With the recent decision by the Federal Circuit establishing that "the Plaintiff bears the burden of establishing proper venue," *In re ZTE, 890 F.3d at 1013*, as opposed to the defendant bearing the burden to establish improper venue, the Court anticipates it will commonly be asked to permit, on motion, a similar, targeted discovery process to ensure it is able to have a complete picture of the underlying venue facts before attempting to apply the statutory requirements of *§ 1400(b)*.

Google's shotgun arguments point in many directions, each intended to persuade that the GGC servers are not places of business within the meaning of the statute: "[t]he GGC servers are standard machines manufactured by a third-party and used to cache static Google content"; "[s]ervers are pieces of equipment, like slot machines or vending machines, and do not rise to the level of being places of business"; "there would be little to no impact to the performance of Google's Edge Network or to Google users if there were no GGC servers **[**37]** in this District," as the "GGC servers in this District are 'a fraction of a fraction' of 1 percent of the total serving capacity of Google's peering and GGC server network." These arguments must be rejected.

In arguing that slot and vending machines are not places of business, Google cites *HomeBingo Network, Inc. v. Chayevsky, 428 F. Supp. 2d 1232, 1250 (S.D. Ala. 2006)* ("That an individual may be a part owner of a piece of equipment (in this case, a slot machine) located in a judicial district does not render the situs of that equipment his regular and established place of business for venue purposes."), and *Magee v. Coca-Cola Refreshments USA, Inc., 833 F.3d 530, 534 (5th Cir. 2016)* (finding that "vending machines are not 'sales establishments,'" where "establishment" was "a place of business or residence with its furnishings and staff."). However, these citations do not support Google's proposition.

First, the Court notes that *HomeBingo* relates to specifically named *individual* (natural person) defendants named in suit in conjunction with a corporate entity. *HomeBingo, 428 F. Supp. 2d at 1235-36*. The specific proposition rejected by the *HomeBingo* Court was that "(i) [the individual corporate officers] Macke, Minard and Chayevsky own, operate, and maintain [the corporate defendant] Cadillac Jack's bingo-based slot machines; (ii) a number of those machines are located at the **[**38]** Atmore casino; and (iii) therefore, Movants have a regular and established place of business in the Southern District of Alabama." *Id. at 1250*. That the proper venue of the corporate defendant, Cadillac Jack's, was properly based upon the presence of the bingo-based slot machines in the Southern **[*955]** District of Alabama was far from being rejected by the *HomeBingo* court—it was *not even challenged by the defendant* in that case. Thus, *HomeBingo* stands for the proposition that Google's GGC server may not establish that Sundar Pichai (Google LLC's CEO) has a regular and established place of business within this District. *Id. at 1251* ("As such, the Court finds that the Cadillac Jack slot machines located at a casino in Atmore, Alabama do not constitute a regular and established place of business for Macke, Minard and Chayevsky, as individuals."). It does nothing to demonstrate that the GGC server should not be considered a regular and established place of business as to Google.

As to *Magee*, the Court first notes that the Fifth Circuit was not considering whether a vending machine was a regular and established place of business but, rather, a "sales establishment" under the ADA such that it constituted a place of "public **[**39]** accommodation" subject to Title III compliance. *833 F.3d at 532*. This is not a beneficial comparison. Further, there are opinions by numerous courts squarely holding that vending machines or similar objects *are* places of business.[32] All

---

[32] *State v. Woods, 242 Ala. 184, 189, 5 So. 2d 732, 736 (Ala. 1942)* ("We may observe, as a matter of common knowledge, that many places of business rent space in their establishments to third persons who may and do conduct their own and different businesses in such space or department so rented. Such space or department becomes, and is, a separate place of business,--the business of such third party. If, therefore, a vending machine owner rents (method of payment immaterial) space for a vending machine and such space becomes his place of business (special or limited), in the conduct of his business he thereby makes himself . . . ."); *Vending Mach. Corp. v. Okla. Tax Comm'n (In re Cigarette Licenses of the Vending Mach. Corp.), 1938 OK 463, ¶ 6, 183 Okla. 427, 429 (1938)* (noting that, in discussing whether two cigarette vending machines in the same location constituted one or two places of business for licensing purposes, "[t]he Legislature has not said that one who sells by means of mechanical devise shall pay more or less than one who sells through the medium of personal salesmanship. It declares that there shall be a separate license for each place of business; and 'place of business,' says the Legislature, 'shall be construed to include the place where orders are received, or where cigarettes are sold.' Then, in the following words, each vending machine is in effect declared to be a place of business: 'Vending machines shall be licensed as a place of business and each and every cigarette vending machine shall have a separate license for each machine from which cigarettes are dispensed.' So far as the classification is concerned, the statute makes no attempt to bring into play any of the usual regulatory measures employed under the police powers. Neither is there an attempt to distinguish or classify upon the basis of volume of business, value of merchandise, capital invested, or mode of dispensing to the trade. . . . In the instant case each vending machine is a complete unit dispensing cigarettes at retail, a complete retail establishment. Each exercises the privilege granted to any other retail dispensary of cigarettes."); *Los Angeles v. Amber Theatres, Inc., 123 Cal. App. 3d 715 n.4, 176 Cal. Rptr. 850, 852 (Cal. Ct. App. 1981)* ("While 'penny arcade' is not defined for zoning

of this **[*956]** aside, it is not the machine alone (be it a server, slot machine, or vending machine) that moves the Court to its ultimate conclusion in this case. It is the server, its physical location within this District, the control exerted over both the server and its location under the GGC agreements (like the Suddenlink Agreement), and the other circumstances here present that lead this Court to conclude these facts meet the strict statutory application laid out by the Federal Circuit in *In re Cray*.

Google's argument relating to the impact of the GGC servers in this District on its Edge Network or on Google users is similarly rejected. The statute does not require "substantial" business or "large" impact from the business being done at the place of business—in order to lay proper venue in a judicial district, the statute simply requires that ***a*** regular and established place of business be present. The Court refuses to read into the statute extra-statutory requirements **[**40]** at the behest of Defendants who have, through their own volition, secured and established multiple places of business within this District.

Google argues that it does not need the GGC servers in this District, and that their contribution to Google's business mission is so small as to be immaterial. However, even the *Personal Audio* court explicitly found that GGC servers may be found in "at least Tyler, Sherman, Plano, and Texarkana," that "[t]he GGC servers carry out a useful role in Google's business, in that they appear to more efficiently connect internet service customers, i.e., customers of Suddenlink or CableOne, to Google content," and that "Google evidently values the contribution of the GGC system." *Personal Audio, 280 F. Supp. 3d at 934* (citations omitted). That the machines are manufactured by third parties is of no moment as places of business are frequently manufactured by third parties. Indeed providing business services, such as office space, logistics, telecommunications, retail and commercial locations, and customer facing automated points-of-sale,[33] ***to*** businesses is not only common but is a business model unto itself. These servers actively service a distinct business need of Google's, as described in the **[**41]** Background section, *supra* at 16. Thus, they are places of business.

Further, the Court has previously seen this "impact" argument in a similar context; it reveals how such a reading of the statute undermines the clear statutory scheme. *See, e.g., Word to Info, Inc. v. Apple Inc.*, 2:17-cv-592-JRG, Apple's Motion to Dismiss for Improper Venue (Redacted Version), Dkt. No. 23 at 4-5[34] (arguing that "Apple's stores do not constitute a regular and established place of business for venue purposes because they account for only a trivial part of Apple's overall business. . . . Apple's two retail **[*957]** stores are not a substantial part of its ordinary business. Apple has approximately 270 retail stores in the United States. The two stores in this district account for less than 1% of Apple's total retail establishments . . . . Likewise, the two stores in this district account for only small part of Apple's sales. Because the two stores in the Eastern District represent such a small part of Apple's overall operations, if Apple closed those stores, its established business . . . would not be appreciably or substantially affected."), at 5 ("Subjecting a company with 80,000

---

purposes in the Municipal Code, Webster's Third New International Dictionary states that HN1 a 'penny arcade' is an amusement center where each device for entertainment may be operated for a penny. The fact that a penny may not be used today to operate these devices has no effect on the basic definition. We would interpret a 'penny arcade,' for zoning purposes, to mean a place of business devoted primarily or in some substantial degree to maintaining coin-operated amusement machines and devices for the purpose of providing public entertainment."); *Hartney Fuel Oil Co. v. Hamer, 2013 IL 115130, ¶ 54, 998 N.E.2d 1227, 376 Ill. Dec. 294, (Ill. 2013)* ("Three additional provisions define 'the seller's place of business' or 'where the seller is engaged in business'" (referencing *86 Ill. Adm. Code 220.115(f)* (sales through vending machines) ("A retailer is engaged in the business of selling food, beverages or other tangible personal property through a vending machine at the location where the vending machine is located when the sale is made if: i) the vending machine is a device operated by coin, currency, credit card, token, coupon or similar device that dispenses food, beverage or other tangible personal property; ii) the food, beverage or other tangible personal property is contained within the vending machine and dispensed from the vending machine; and iii) the purchaser takes possession of the purchased food, beverage or other tangible personal property immediately.)).

[33] For example: unattended gas pumps, vending machines, automated car washes, bike share kiosks, etc. *See also* Automated Retail, Wikipedia (*available at* https://en.wikipedia.org/wiki/Automated_retail).

[34] The Court recognizes that Apple has recently urged similar arguments in a currently pending motion, *Alert Signal Intellectual Property, LLC v. Apple Inc.*, No. 2:18-cv-177-JRG, Apple's Motion to Dismiss for Improper Venue (Redacted Version), Dkt. No. 19 at 1, 5. The above argument is presented for illustration and the Court does not prejudge Apple's motion here. The Court will fully analyze and address those arguments in their entirety when that motion is ripe.

employees and 270 stores **[**42]** across the United States to venue in the Eastern District because of the presence of two retail outlets accounting for only [redacted] of Apple's revenues would allow the tail to wag the dog, especially when those stores do not represent the totality of Apple's business operations."). Examining the "effect" on a company's business which a particular place or places of business have is not in keeping with a strict statutory application. In fact, it undermines it. Reading a non-statutory requirement that the place of business for *§ 1400(b)* requires the place of business to be a substantial part of a defendant's ordinary business or have a material effect on a business's provisioning of goods or services does violence to the language of the statute and is precisely the kind of statutory deviation the Federal Circuit cautioned against in *In re Cray. 871 F.3d at 1362* ("We stress that the analysis must be closely tied to the language of the statute."), *1364, n. 1* (noting that any "relative comparison" of "the nature and activity of the alleged place of business of the defendant in the district in comparison with that of other places of business of the defendant in other venues" should not include "value judgments on the **[**43]** different types of business activity conducted therein.") (emphasis omitted).

Google additionally argues that "the servers are also not 'regular and established' because under the agreements between Google and the ISPs, either party can terminate at any time and for any reason." (Dkt. No. 125 at 11 (citing the Suddenlink Agreement)). The Court disagrees. A business which has a five-year agreement is certainly no less established with a month remaining on the lease than it is in the first year of the lease. A month-to-month agreement which has endured for years is clearly "regular and established." There is little question that Google intends the GGC servers to be a "[s]calable long term solution for edge content distribution," and it is undisputed that they have been such a solution in this District for years. (Dkt. No. 141-18 (Mike Axelrod, The Value of Content Distribution Networks and Google Global Cache) at 10; Dkt. No. 141 at 19). The fact that the Suddenlink Agreement may be terminated is not evidence that Google's presence in this District is somehow less than "regular and established." Few sophisticated transactional documents fail to have one or more escape clauses, but nothing about such provisions makes the **[**44]** commercial targets addressed less than established.

As a part of ensuring a proper application of the statutory language, it may be appropriate to consider similar types of places of business to demonstrate the appropriateness of this Court's finding. SEVEN argues that "GGC servers in the Edge Nodes function as local data warehouses, much like a shoe manufacturer might have warehouses around the country. Instead of requiring people to obtain information from distant Core Data Centers, which would introduce delay, Google stores information in the local GGC servers to provide quick access to the data." (Dkt. No. 141 at 4). "The only relevant difference between a warehouse that stores a company's tangible products and **[*958]** Google's GGC servers is the nature of the products being stored—physical merchandise versus digital content. Regardless of what the products may be, if the physical structure that stores them is 'a physical, geographical location in the district from which the business of the defendant is carried out,' that structure is a place of business under *§ 1400(b)*." (*Id.* at 15 (citing *In re Cray, 871 F.3d at 1362*)). The Court agrees.

There is no question that warehouses are properly considered places of business and have been **[**45]** so held, by both legislatures and courts.[35] ,[36] ,[37] This recognition makes **[*960]** intuitive sense. The vast majority of business organizations require and utilize some form of storage or logistics. Of course, businesses may store items at *other* business's locations (like, for

---

[35] *State v. Hutton, 39 Mo. App. 410, 416 (Mo. Ct. App. 1890)* ("This act, as amended by the act of March 24, 1887, recites: 'No such license shall authorize any merchant to sell vinous, fermented or spirituous liquors in any quantities, to be drank **at his store, stand or warehouse, or other place of business**.'") (quotation omitted) (emphasis added); *Kansas City v. Butt, 88 Mo. App. 237, 238 (Mo. Ct. App. 1901)* ("that defendant, as manager of said corporation, was engaged in the manufacture and production of ice by artificial means; that **no place of business, depot or warehouse was kept for the selling of ice**.") (emphasis added); *Gregory v. Wabash Ry. Co., 46 Mo. App. 574, 577 (Mo. Ct. App. 1891)* ("Hutchinson on Carriers, section [89], thus clearly states the law: . . . 'But, **if the delivery be made at the warehouse or other place of business of the carrier** for as early transportation as can be made in the course of the carrier's business, and subject to only such delays as may necessarily occur in awaiting the departure of trains, . . . or from the performance of prior engagements by him, he becomes, the moment the delivery is made, a carrier as to the goods, and his responsibility as such at once attaches.'") (citation omitted) (emphasis added); ***Woods v. Postal Telegraph-Cable Co., 205 Ala. 236, 241, 87 So. 681, 685 (1920)*** ("'improvements,' as used in a lease which provided that all improvements of the building shall belong to the landlord at the expiration of the term, may be said to 'comprehend everything that tends to add to the value or convenience of **a building or a place of**

example, Fulfillment by Amazon[38]) wherein goods are stored by third parties at the third parties' discretion and with no control over the location, management, or daily supervision of the products in storage. Such an arrangement can scarcely be considered to render the physical location of the stored items a place of business as to the party whose goods are stored. However, were that same party to integrate the storage arrangement into its own logistical operations (similar to, for example, Amazon and its relationship with its own fulfillment centers), there can be little doubt that the storage warehouses are places of business, *even if the public never interacts with the warehouse. See* Smith v. Farbenfabriken of Elberfeld Co., 203 F. 476, 479-81 (6th Cir. 1913).[39]

Here, the GGC servers are best characterized as local data warehouses, storing information in local districts to provide Google's users with quick access to the cached data, avoiding the delays associated with distant data retrieval from Google Data Centers. (Dkt. No. 141 at 4). This **[*961]** type of logistical positioning is commonplace for larger corporate interests, especially where prompt delivery is a core aspect of a business strategy.[40] ,[41] This is the case with **[**48]** Google.[42] Holding that Google's business done at and through the GGC servers faithfully comports with the language of the statute; it is the logical result this Court has reached.[43]

In considering the language of the patent venue statute, some courts have held that § 1400(b) "requires some employee or agent of the defendant to be conducting business at the location in question." Peerless **[*962]** Network, Inc. v. Blitz Telecom Consulting, LLC, No. 17-CV-1725 (JPO), 2018 U.S. Dist. LEXIS 49628, 2018 WL 1478047, at *4 (S.D.N.Y. Mar. 26, 2018).[44] These cases

---

business, [46] whether it be a store, manufacturing establishment, warehouse, or farming premises**.'") (citation omitted) (emphasis added); City of Newport v. French Bros. Bauer Co., 169 Ky. 174, 183 S.W. 532, 534 (Ky. 1916) ("the appellee at no time ever had any goods not sold previous to the time of delivery in Kentucky, and had never maintained **any warehouse, storeroom, or other place of business** in Kentucky") (emphasis added); Hasselbring v. Koepke, 263 Mich. 466, 480, 248 N.W. 869, 873 (Mich. 1933) ("In other words, the nature and extent of the right is to have that amount of light through the windows of the dominant house which is sufficient, according to the ordinary notions of mankind, for the comfortable use and enjoyment of the house as a dwelling-house, if it be a dwelling-house, or for the beneficial use and occupation of **the building if it be a warehouse, shop, or other place of business**.") (citing 11 Halsbury's Laws of England, p. 300) (emphasis added); Huebner-Toledo Breweries Co. v. Mathews Gravity Carrier Co., 253 F. 435, 442, 1919 Dec. Comm'r Pat. 251 (6th Cir. 1918) ("Palmer obtained a patent in 1888, No. 376,340, on an elevator, which may properly be regarded as a distributing contrivance; it was designed for carrying goods or other materials up or down **in a warehouse, store, manufactory, or other similar place of business**.") (emphasis added); J.B. Van Sciver Co. v. Flurer, 11 N.J. Misc. 464, 167 A. 513, 513 (N.J. Dist. Ct. 1933) ("**It maintains no warehouse, factory, general offices, or other place of business outside the state of New Jersey**") (emphasis added); Wagner v. City of Covington, 177 Ky. 385, 197 S.W. 806, 807 (Ky. 1917), aff'd, 251 U.S. 95, 40 S. Ct. 93, 64 L. Ed. 157, 17 Ohio L. Rep. 437 (1919) ("**appellants have no warehouse or other place of business in Covington**") (emphasis added); Hill Mfg. Co. v. New Orleans, M. & C.R.R. Co., 117 Miss. 548, 78 So. 187, 191 (Miss. 1918) ("The rule is stated in section 113 of Hutchinson on Carriers, vol. 2, as follows: 'But if the delivery be made **at the warehouse or other place of business of**

reason that this must be so since, to be a place of business, "the defendant must actually engage in business from that location," such that, "for example, products are made, customers are served, or business decisions are made." *Id.* However, this requirement finds no basis within the language of the statute, nor does it accord with conceptions of places of business stretching back to at least the turn of the 20th century. **[**49]** *See, e.g., supra* at 31 n.35, 32 n.36. The mandates of *In re Cray* requiring that a court's "analysis must be closely tied to the language of the statute" prevents both the removal of statutory requirements and the addition of extra-statutory requirements with equal force. *871 F.3d at 1362*; *see also* *Fed. Elec. Prods. Co. v. Frank Adam Elec. Co., 100 F. Supp. 8, 10-11 (S.D.N.Y. 1951)* ("Lengthy precedent is available to show that courts have been unwilling to constrict the definition of 'regular and established place of business.'"); *Urquhart v. American-La France Foamite Corp., 144 F.2d 542, 543 n.3, 79 U.S. App. D.C. 219, 1944 Dec. Comm'r Pat. 82 (D.C. Cir. 1944)*, cert. denied *323 U.S. 783, 65 S. Ct. 273, 89 L. Ed. 625 (1944)* ("Nor should the term 'a regular and established place of business' be narrowed or limited in its construction.") (citing *Shelton v. Schwartz, 131 F.2d 805, 808 (7th Cir. 1942))*; *Shelton, 131 F.2d at 809* ("Emphasis must be on the existence of the regular and established place of business,—not on the nature or character of the business conducted there.").

Any such addition or subtraction from the language of the statute is improper and contrary to the express prohibition as set forth in *In re Cray*. "[T]he requirement of venue is specific and unambiguous; it is not one of those vague principles which, in the interests of some overriding policy, is to be given a liberal construction." *In re ZTE, 890 F.3d at 1014* (citing *In re Cray, 871 F.3d at 1361*). The narrowing would do violence to the plain

---

the carrier for as early transportation as can be made in the course of the carrier's business, . . . he becomes, the moment the delivery is made, a carrier as to the goods") (emphasis added); *Wingfield v. Kutres, 136 Ga. 345, 71 S.E. 474, 475 (Ga. 1911)* ("Section 2 prescribed a license fee of $500 for each calendar year or part thereof to be paid by every person, firm, or corporation who shall maintain **a supply depot, warehouse or distributing offices or other place of business** within the limits of this state") (emphasis added); *Inhabitants of Abington v. Inhabitants of N. Bridgewater, 40 Mass. 170, 177, 23 Pick. 170 (Mass. 1839)* ("**if it be his place of business, he may have a warehouse, manufactory, wharf or other place of business, in connexion with his dwellinghouse in different towns**.") (citing *Lyman v. Fiske, 34 Mass. 231, 231, 17 Pick. 231 (Mass. 1835))* (emphasis added); *Flynn v. Colonial Disc. Co., 149 Misc. 607, 610, 269 N.Y.S. 394 (City Ct. 1933)* ("**His storage room is in effect as much a part of his place of business as is his showroom. A sale from his warehouse is in fact a sale 'in the ordinary course of business**.'") (emphasis added); *Grantham v. City of Chickasha, 1932 OK 123, 156 Okla. 56, 9 P.2d 747, 748 (Okla. 1932)* ("The ordinance, in part, provides as follows: 'Ordinance No. 1032. . . . Section Two (2): . . . That the term itinerant merchant as herein used in this ordinance, shall be deemed to mean and include any and all itinerant vendors, . . . who have no fixed or established **store, warehouse, or other place of business** within the City of Chickasha.'") (emphasis added); *Morgan v. State, 140 Ga. 202, 78 S.E. 807, 807 (Ga. 1913)* ("The Court of Appeals has certified to the Supreme Court the following question[]: . . . Is the said act in conflict with the ***fourteenth amendment of the Constitution of the United States*** in that: (a) The act imposes a greater tax upon persons maintaining '**a supply depot, warehouse, distributing office, or other place of business** within this state . . .'") (emphasis added). *In re BigCommerce, 890 F.3d at 983 (Fed. Cir. 2018)* (approving of "the general principle of statutory construction that 'where words are employed in a statute which had at the time a well-known meaning at common law or in the law of this country, they are presumed to have been used in that sense unless the context compels to the contrary.") (citing *Standard Oil Co. v. United States, 221 U.S. 1, 59, 31 S. Ct. 502, 55 L. Ed. 619 (1911)*.

[36] This common view of warehouses as places of business continued throughout the 20th century. *See, e.g., Fed. Elec. Prod. Co. v. Frank Adam Elec. Co., 100 F. Supp. 8, 10 (S.D.N.Y. 1951)* ("**Defendant has a number of what it terms 'reshipping centers' spaced around the country**. One of these is located in New York City. Defendant describes its function as 'incidental to the filling of orders for goods manufactured and sold in Missouri, by expediting delivery thereof to purchasers along the Atlantic Seaboard.' It denies that the New York operation constitutes a regular and established place of business within the meaning of *Section 1400(b)*. . . . The mechanics of bookkeeping which invoiced these orders in St. Louis, do not alter the nature of defendant's New York office. **It is a regular and established business within the meaning of *Section 1400(b)***.") (emphasis added); *New Wrinkle v. Fritz, 30 F. Supp. 89, 90-91 (W.D.N.Y. 1939)* ("Defendant corporation's plant is located at Pontiac, Michigan. It has no office for the transaction of business in this district. **It has no warehouse [**47] within this district. . . . The foregoing facts do not show that the defendant corporation has 'a regular and established place of business' in this district.**") (emphasis added); *E. H. Sheldon & Co. v. Norbute Corp., 228 F. Supp. 245, 246-47 (E.D. Pa. 1964)* ("Neither defendant nor Metalab owns, leases or otherwise controls **any office, warehouse or other permanent location in this district**. . . . In the present case the defendant does not maintain, control or pay for an establishment in this district. **It has no regular and**

language of the statute, as § 1400(b) does not require that the place of business ***also be*** a place of employment by **[**50]** the defendant.[45]

Recent legislation also reveals the impropriety of the imposition of an extra-statutory human-centric requirement. The *Leahy-Smith America Invents Act, P.L. 112-29,*, ("the AIA") was enacted September 16, 2011. It is widely considered to be "a change at least as significant for this Nation's patent system as the formation of the Federal Circuit in 1982." Synopsys, Inc. v. Mentor Graphics Corp., 814 F.3d 1309, 1324 (Fed. Cir. 2016) (Newman, J., dissenting), overruled by Aqua Prods., Inc. v. Matal, 872 F.3d 1290 (Fed. Cir. 2017). The AIA "is the product of extensive study by the concerned communities and the Congress," and the breadth of its reach in reforming facets of patent law, both substantive and procedural, is unquestionably vast. Id. at 1325. Of note, Congress enacted, but did not codify, Section 18 of the AIA, **[*963]** which established a "Transitional Program for Covered Business Method Patents." *P.L. 112-29, Sec. 18*. This Section set up an additional post-grant proceeding, Covered Business Method Review, in addition to the two codified options created by the AIA, Post-Grant Review and *Inter Partes* Review. Of special interest to applications of § 1400(b), the Section reached beyond the confines of the newly

---

established place of business here. The suit, therefore, cannot be maintained here.") (emphasis added); Holub Indus., Inc. v. Wyche, 290 F.2d 852, 853 (4th Cir. 1961) ("**It has no regular or established place of business or office or warehouse of any kind in South Carolina** and is not registered to do business in that state.") (emphasis added); Brevel Prod. Corp. v. H & B Am. Corp., 202 F. Supp. 824, 827 (S.D.N.Y. 1962) ("An essential prerequisite for a finding of venue in cases of this sort is that the defendant actually maintains, in the words of the statute, 'a regular and established place of business' within the district. **This 'place of business' can be a branch office, a sales-showroom, or a warehouse o[r] distribution center**. But it must be maintained and paid for by the defendant. The mere fact that defendant hires a sales representative who in turn rents offices to sell defendant's products is insufficient.") (citations omitted) (emphasis added). Indeed, warehouses are commonly viewed as "integral" to the conduct of business and business purposes. *See, e g.,* In re McCrary's Farm Supply, Inc., 705 F.2d 330, 334 (8th Cir. 1983) ("Employees of Central Terminal Warehouse did not solicit business for McCrary's. They did, however, perform stock transfers for McCrary's and assist in making merchandise available for pick up either by McCrary's, its customers, or common carriers. Sales involve more than simply solicitation, and **we are satisfied that Central Terminal, in contributing to the storage and distribution of merchandise, performed an integral part of McCrary's sales activity and business**.") (emphasis added).

[37] *But see* CDx Diagnostic, Inc. v. United States Endoscopy Grp., Inc., No. 13-CV-5669(NSR), 2018 U.S. Dist. LEXIS 87999, 2018 WL 2388534, at *3 (S.D.N.Y. May 24, 2018) ("[S]torage units are not 'regular and established places of business', because Plaintiffs have failed to demonstrate that Defendant 'actually engage[s] in business from [either] location.' The question is whether the storage units are 'location[s] at which one carries on a business.' They are not. While Defendant's customer service reps may 'typically' retrieve materials from the storage units to visit customers within this District, no 'employee or agent of [Defendant actually] conduct[s] business at' the storage units, whatsoever.") (citations omitted).

[38] See https://services.amazon.com/fulfillment-by-amazon/benefits.html ("With Fulfillment by Amazon (FBA), **you store your products in Amazon's fulfillment centers**, and we pick, pack, ship, and provide customer service for these products."); *see also* Amazon.com, Inc., 2017 Annual Report at 3 ("We offer programs that enable sellers to grow their businesses, sell their products on our websites and their own branded websites, and fulfill orders through us. We are not the seller of record in these transactions. We earn fixed fees, a percentage of sales, per-unit activity fees, interest, or some combination thereof, for our seller programs."); *id*. at 8 ("Under some of our commercial agreements, we maintain the inventory of other companies, thereby increasing the complexity of tracking inventory and operating our fulfillment network.").

[39] Id. at 479 (holding a mail order drug business, run from a residence in Windsor, Canada, but with a warehouse in Detroit, Michigan, with "All orders filled promptly and completely from [the] Detroit warehouse, duty paid," is a regular and established place of business for purposes of venue in a patent case, even though the warehouse "does not receive orders directly from customers or enter into contracts with them, or receive any money in payment of bills; and . . . has no authority so to do."), at 480-81 ("If what is done at the warehouse at Detroit, and in that city, looking to the delivery of the goods, were subtracted from what is done in Windsor, appellant could not conduct his present business at all. We need not repeat that he has no other warehouse, no other representative, and no stock of goods through which to conduct business, except only at the Woodward avenue warehouse in Detroit. Now, despite the fact that the preliminary steps are taken at Windsor, it is plain enough that the final and essential acts of infringement in issue are committed by [a warehouse employee] at the warehouse in Detroit, and through his dealings with the carriers at the warehouse and elsewhere within that city. [The warehouse employee] thus does something with respect to the business upon which the suit is founded. [The warehouse employee] is

enacted law to *specifically exempt* a particular regular and established place of business for purposes **[**51]** of venue under *§ 1400(b)*. Section 18(c) reads as follows:

> ATM EXEMPTION FOR VENUE PURPOSES.--In an action for infringement under *Section 281 of title 35, United States Code*, of a covered business method patent, an automated teller machine shall not be deemed to be a regular and established place of business for purposes of *section 1400(b) of title 28, United States Code*.

Accordingly, Congress specifically withdrew automated teller machines ("ATMs") from those regular and established places of business which could be used to establish venue.[46] A plain reading of this exception indicates that ATMs and similar devices *would otherwise constitute regular and established places of business. See also* Edward D. Manzo, America Invents Act: A Guide to Patent Litigation and Patent Procedure, Venue, America Invents Act § 17:12 (2017).[47]

"Courts assume that a legislature always has in mind previous statutes relating to the same subject when it enacts a new provision. In the absence of any express repeal or amendment, the new provision is presumed to accord with the legislative policy embodied **[**52]** in those prior statutes, and they all should be construed together." 2B Sutherland Statutory Construction § 51:2 (7th ed.); *accord* A. Scalia & B. Garner, READING LAW 252 (2012) ("Any word or phrase that comes before the Court for interpretation . . . . is part of an entire *juris corpus*. So, if possible, it should no more be interpreted to clash with the rest of that corpus than it should be interpreted to clash with other provisions of the same law."); *Goodyear Atomic Corp. v. Miller, 486 U.S. 174, 184-85, 108 S. Ct. 1704, 100 L. Ed. 2d 158 (1988)* ("We generally presume that Congress is knowledgeable about existing law pertinent to the legislation it enacts."). "Statutes cannot be read intelligently if the eye is closed to considerations evidenced in affiliated statutes." Felix Frankfurter, *Some Reflections on the Reading of Statutes*, 47 COLUM. L. REV. 527, 539 (1947). "It is well established **[*964]** in the statutory field that unless the context indicates otherwise, words or phrases in a provision that were used in a prior act pertaining to the same subject matter will be construed in the same

---

there in the right of appellant, and [The warehouse employee]'s acts are appellant's acts; and to say that appellant has 'no regular and established place of business' there is to ignore the use that has been made for years of the Woodward avenue warehouse.").

[40] *See, e.g.*, Lisa Fickenscher, "Amazon is finally opening one of its mega-warehouses in New York" (June 19, 2017) (*available at* https://nypost.com/2017/06/19/new-yorkers-are-getting-faster-shipping-thanks-to-amazon/, accessed on July 11, 2018) ("Amazon's ability to quickly ship stuff to New Yorkers, from Kindle readers to kayaks, is about to get a major boost. . . . The Amazon 'fulfillment center' will span nearly 1 million square feet on the west shore of Staten Island, amping up Amazon's access to millions of online shoppers in Manhattan, Brooklyn, Queens and Long Island, sources close to the situation said. . . . In December 2014, Amazon opened a 40,000-square-foot 'Prime Now' hub — **filling urgent orders for beer, shampoo and printer cartridges within a few hours with the help of bike couriers** — at 7 W. 34th St. in Manhattan.").

[41] This type of close storage location is seen in a variety of fields and industries. *See, e.g.*, Dept. of Energy, Strategic Petroleum Reserve Storage Sites (*available at* https://www.energy.gov/fe/services/petroleum-reserves/strategic-petroleum-reserve/spr-storage-sites) ("Storage locations along the Gulf Coast were selected because they provide the most flexible means for connecting to the Nation's commercial oil transport network. Strategic Reserve oil can be distributed through interstate pipelines to nearly half of the Nation's oil refineries or loaded into ships or barges for transport to other refineries."); Edward T. O'Donnell, *The Dawn of New York's Ice Age*, N.Y. Times (July 31, 2005) (*available at* https://www.nytimes.com/2005/07/31/nyregion/thecity/the-dawn-of-new-yorks-ice-age.html) ("1855 . . . brought the incorporation of the Knickerbocker Ice Company, an enterprise that quickly became the city's largest supplier. Knickerbocker developed a massive ice harvesting operation at Rockland Lake in Nyack and along the banks of the upper Hudson River, and during the winter months it employed thousands of men to cut huge blocks of ice and haul them to scores of large ice warehouses. When the warm weather set in, barges carried the product to the Manhattan docks, where it was transferred to icehouses dotted around the city and then distributed to customers via ice wagons.").

[42] *See* Alphabet, Inc., 10-K (2017 fiscal year) (*available at* https://abc.xyz/investor/pdf/20171231_alphabet_10K.pdf) at

sense." *Texaco, Inc. v. Dep't of Energy, 795 F.2d 1021, 1030 (Temp. Emer. Ct. App. 1986)* (citation and internal quotations omitted).[48]

Automated Teller Machines are not operated, in person or remotely, by employees of the owning financial institution.[49] Any reading of the statutory requirements

propelling new ideas and people forward. At Google, our mission is to make sure that information serves everyone, not just a few. So whether you're a child in a rural village or a professor at an elite university, you can access the same information. We are helping people get online by tailoring digital experiences to the needs of emerging markets. **We're also making sure our core Google products are fast and useful, especially for users in areas where speed and connectivity are central concerns**.").

[43] The Court notes with interest the ironic positions Google takes in its Motion. While clearly taking the position that "Servers are pieces of equipment . . . and do not rise to the level of being places of business," (Dkt. No. 125 at 10-11), it also represents that "the Google applications and services named in the Complaint *are provided by Google servers* in Google data centers located outside this District." (*Id.* at 17). Google continues, stating that the alleged infringement *by Google*, cannot have occurred within this District because "Google has no data centers in this District." (*Id.* at 18-19). Google cannot argue that it both does business at and through servers in its data centers while plausibly maintaining that servers themselves cannot be places of business.

[44] At argument on this Motion, Google went further, refusing to concede that a place with Google employees present at it constituted proper venue under the statute. (Dkt. No. 193, Hr'g Tr. at 20:4-12 ("THE COURT: If Google has a place with employees present, is it subject to venue there? MR. VERHOEVEN: That'd be a much closer call, Your Honor. It would depend specifically on the facts and circumstances. Certainly, if Google had an office that had a sign on it and people could walk in, customer - or business customers could walk in, not necessarily retail people -- or retail people, then that would be - probably be a place of business.").

[45] *See Place of Employment*, BLACK'S LAW DICTIONARY (10th ed. 2014) ("The location at which work done in connection with a business is carried out; the place where **some process or operation** related to the business is conducted.") (emphasis added).

[46] Interestingly, this result was not as broad as the financial services industry proposed. *See Patent Reform: The Future of American Innovation: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 291 (2007) (Testimony of John A. Squires on behalf of the American Bankers Assn., et al.) (commenting on the Patent Reform Act of 2007 (which redefined "resides" for *§ 1400(b)* to exclude the definition found in *§ 1391(c)*), and arguing that "[i]t is appropriate to create a test whereby both parties have [a] substantial business nexus in the judicial district or otherwise constrained by this statute. Financial firms do not want to be open to suit in any and all districts due simply to the presence of a branch or an ATM."). Even so, at least one commentator views this limited exemption as a "bank bailout." Lawrence A. Kogan, *Commercial High Technology Innovations Face Uncertain*

53 ("We generate revenues primarily by delivering relevant, cost-effective online advertising"), at 4 ("The goal of our advertising business is to deliver relevant ads at just the right time and to give people useful commercial information, regardless of the device they're using."), at 3 ("The Internet is one of the world's most powerful equalizers, capable of

of § 1400(b) that **[**53]** inserts an extra-statutory requirement of human-centric activity at the "regular and established place of business" necessarily renders this express exemption superfluous. A. Scalia & B. Garner, READING LAW 174 (2012) ("The surplusage canon holds that it is no more the court's function to revise by subtraction than by addition."). A "cardinal principle of statutory interpretation" is that no provision "shall be superfluous, void, or insignificant." TRW Inc. v. Andrews, 534 U.S. 19, 31, 122 S. Ct. 441, 151 L. Ed. 2d 339 (2001); Gustafson v. Alloyd Co., 513 U.S. 561, 574, 115 S. Ct. 1061, 131 L. Ed. 2d 1 (1995) ("[T]he Court will avoid a reading which renders some words altogether redundant."); Mountain States Tel. & Tel. Co. v. Pueblo of Santa Ana, 472 U.S. 237, 249, 105 S. Ct. 2587, 86 L. Ed. 2d 168 (1985) (applying the "elementary canon of construction that a statute should be interpreted so as not to render one part inoperative") (citation omitted). Where "one statute deals with a subject in general terms and another deals with a part of the same subject in a more detailed way, the two should be harmonized if possible." 2B Sutherland Statutory Construction § 51:5 (7th ed.). A. Scalia & B. Garner, READING LAW 181 (2012) ("[T]here can be no justification for needlessly rendering provisions in conflict if they can be interpreted harmoniously."). Where two acts are *in pari materia*, as here, they should be construed together. But even if one reads the ATM exemption **[**54]** of AIA Sec. 18(c) as being in conflict with the generally application of the special venue statute, "the general statute must yield to the specific statute involving the same subject, regardless of whether it was passed prior to the general statute." 2B Sutherland Statutory Construction § 51:5 (7th ed.); Morton v. Mancari, 417 U.S. 535, 550-51, 94 S. Ct. 2474, 41 L. Ed. 2d 290 (1974) (Blackmun, J.) ("Where there is no clear intention otherwise, a specific statute will not be controlled or nullified by a general one, regardless of the priority of enactment.") (citing Bulova Watch Co. v. United States, 365 U.S. 753, 758, 81 S. Ct. 864, 6 L. Ed. 2d 72, 1961-1 C.B. 782 (1961); Rodgers v. United States, 185 U.S. 83, 87-89, 22 S. Ct. 582, 46 L. Ed. 816, 37 Ct. Cl. 552 (1902)). Accordingly, the Court holds that the "regular and established place of business" requirement of § 1400(b) does not countenance the addition of a further human-centric requirement at the place of business.

Having so held, the Court finds that, for the reasons discussed above, the GGC servers and their several locations within this District constitute "regular and established place[s] of business" within the meaning of the special patent venue statute.

[*965] *iv. Of the Defendant*

The last of the three statutory requirements identified by the Federal Circuit in *In re Cray* is that the regular and established place of business be "of the defendant." 871 F.3d at 1362-63. Other courts have previously found "shelves" which store telecommunications equipment **[**55]** are "places of the defendant." Peerless Network, 2018 U.S. Dist. LEXIS 49628, 2018 WL 1478047, at *3 ("[A]ssuming that Local Access rents the shelf on which its equipment rests, the Court is satisfied that the shelf is 'a place of the defendant,' even if the shelf is figuratively land-locked inside of Peerless territory. The fact that Local Access employees must gain Peerless's permission to visit their shelf does not change the fact that, as alleged, the shelf belongs to Local Access.") (internal citations omitted). This case presents a similar situation[50] and thus reaches a similar

---

Future Amid Emerging "Brics" Compulsory Licensing and IT Interoperability Frameworks, 13 San Diego Int'L L.J. 201, 300 (2011) (noting "the provision in the [AIA] excluding ATM machines as a venue tool") (citing AIA Sec. 18(c)).

[47] H.R. REP. NO. 112-98, pt. 1, at 81 (2011) ("Subsection (c) deems that in an action for infringement under § 281 of a covered business method patent, an automated teller machine ('ATM') shall not be considered a regular and established place of business for purposes of the patent venue statute.") (citing 28 U.S.C. § 1400(b)).

[48] The precedent of the Temporary Emergency Court of Appeals, eventually replaced by the Court of Appeals for the Federal Circuit, has been adopted by the Court of Appeals for the Federal Circuit to some extent. *See* Tex. Am. Oil Corp. v. United States Dep't of Energy, 44 F.3d 1557, 1561 (Fed. Cir. 1995) (en banc) ("[T]he Court of Appeals for the Federal Circuit adopts as precedent the body of law represented by the holdings of the Temporary Emergency Court of Appeals."); *but see* Marriott Int'l Resorts, L.P. v. United States, 437 F.3d 1302, 1306 n.4 (Fed. Cir. 2006).

[49] Hence, "automated."

[50] (*See* Dkt. No. 193, Hr'g Tr. at 20:17-22 ([MR. VERHOEVEN:] "In this case, there are no Google employees. In fact, there's no record that any Google employee has ever been to any of the ISPs identified by SEVEN in this motion. Google employees don't have access. They'd have to get permission to enter."), at 23:3-7 ([MR. VERHOEVEN:] "Google owns the servers. Google owns the software. Google controls what can be done with the servers. It doesn't control what rack they're put on. But it -- but it does control -- they can't open up

result.

Google argues that "the rooms and buildings that house the GGC servers in this District . . . are not Google's." (Dkt. No. 125). The Court recognizes that they may not, on their own, establish proper venue as to Google in this District. *See* Personal Audio, 280 F. Supp. 3d at 934 ("The property on which they are located is not owned, leased, or controlled by Google. The 'server rooms' are not rooms from which the business of Google is conducted.").

However, as discussed above, *supra* Part III.B.ii., the "place" of the "place of business" is not the room or building of the ISP but rather Google's server and the space wherein it is located. There is little doubt that both the server and the physical location **[**56]** in and at which it resides is under the exclusive control of Google. The rack space allotted for the GGC server is "provided" to Google. (Dkt. No. 141-23 at 6 ("Space: The Host shall provide Google rack space for the Equipment located at the Space within Host premises."). The precise location of that space, and thus the server, is reported to Google by the ISP. (Dkt. No. 141-23 at 3 ("Contact & Location Details: As soon as practicable after the Effective Date, the parties will advise each other in writing (which may be sent electronically) of the following: . . . (c) Equipment location (address/floor/rack)")). Further, as noted *supra* at 22-23, "Google's ownership of the server and its contents is absolute, as is its control over the server's location, once installed." (*See* Dkt. No. 141-23 at 6). Google's ownership of the server and control thereof has not been a focus of Google's objections to proper venue in this District. *Supra* at 24 n 30.

Google itself has denoted that the GGC servers are places "of Google." As the Federal Circuit instructed in *In re Cray*, "a defendant's representations that it has a place of business in the district are relevant." 871 F.3d at 1363. In this respect, "[p]otentially relevant inquiries include whether the **[**57]** defendant lists the alleged place of business on a website," in determining whether "the defendant [has] establish[ed] or ratif[ied] the place of business," within the meaning of the statute. *Id.* Here, Google has done so. Google states on http://peering.google.com that "Our Edge Network is how we connect with ISPs to get traffic to and from users" **[*966]** and that this content traffic "can come from multiple *Google locations, including our data centers Edge PoPs, and* ***Edge Nodes***." (Dkt. No. 197-1 at 1).[51]

The Court concludes that the GGC servers and their locations within the various ISPs within this District are "places of Google" sufficient to meet the statutory requirement of § 1400(b).

IV. Conclusion

In light of the foregoing, the Court finds and holds that:

1) SEVEN has adequately pleaded acts of infringement within this District sufficient to meet the requirements of 28 U.S.C. § 1400(b). *Supra* at 14.

2) SEVEN has met its burden of demonstrating that the GGC server and its location is a "physical place" within the meaning of § 1400(b). *Supra* at 24.

3) SEVEN has met its burden of demonstrating that the GGC server and its location is a "regular and established **[*967]** place of business" within the meaning of § 1400(b).[52] *Supra* at 39.

4) SEVEN has met its burden of demonstrating **[**58]** that the GGC server and its location is a "place of the defendant" within the meaning of § 1400(b). *Supra* at 41.

Having so found, the Court holds that the statutory

---

these servers. They can't mess with them.")).

[51] Additional statements from that website further confirm the ratification by Google. (*See* Dkt. No. 141-13 at 2 ("Google's network infrastructure has three distinct elements: Core data centers, Edge Points of Presence (PoPs), Edge caching and services nodes (Google Global Cache, or GGC)"), at 5 ("Edge nodes (Google Global Cache, or GGC) Our edge nodes (called Google Global Cache, or GGC) represent the tier of Google's infrastructure closest to our users. With our edge nodes, network operators and internet service providers deploy Google-supplied servers inside their network. Static content that is very popular with the local host's user base, including YouTube and Google Play, is temporarily cached on edge nodes. Google's traffic management systems direct user requests to an edge node that will provide the best experience. In some locations, we also use our edge nodes to support the delivery of other Google services, such as Google Search, by proxying traffic where it will deliver improved end-to-end performance for the end user."). Google also presents a "[m]ap of metros where at least one Edge node (GGC) is present," *id.*, which identifies the GGCs located at least in Tyler and Sherman. (Dkt. No. 141 at 24 (citing Dkt. No. 141-13)). A portion of this map has been reproduced below (with the yellow dot west of Tyler indicating the presence of the

requirements of § 1400(b) are met in this case and that venue is proper as to Google within this District.[53] Accordingly, the Court hereby **DENIES** Google LLC's Second Renewed Motion to Dismiss or, in the Alternative, Transfer under 28 U.S.C. § 1406 for Improper Venue. (Dkt. No. 125).

It is further **ORDERED** that this ruling will remain **PROVISIONALLY SEALED** until the Parties file joint proposed redactions, with specific explanations for the necessity of such redactions, within seven (7) days of this order, after which a redacted version will be entered by the Court.

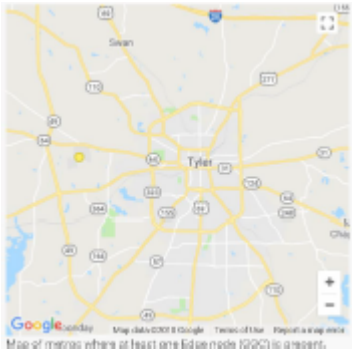
So ORDERED and SIGNED this 19th day of July, 2018.

/s/ Rodney Gilscrap

RODNEY GILSCRAP

UNITED STATES DISTRICT JUDGE

End of Document

Edge node (GGC)): 

[52] With regard to a current analysis of what constitutes "business" within the language of the statute, recent guidance from the Supreme Court appears to caution against ignoring the state of the modern economy. S. Dakota v. Wayfair, Inc., 138 S. Ct. 2080, 2093, 201 L. Ed. 2d 403 (2018) ("[T]he Court should focus on rules that are appropriate to the twenty-first century, not the nineteenth.") (citations and internal quotations omitted), at 2095 ("[I]t is not clear why a single employee or a single warehouse should create a substantial nexus while 'physical' aspects of pervasive modern technology should not."), at 2095 ("The 'dramatic technological and social changes' of our 'increasingly interconnected economy' mean that buyers are 'closer to most major retailers' than ever before—'regardless of how close or far the nearest storefront.' Between targeted advertising and instant access to most consumers via any internet-enabled device, 'a business may be present in a State in a meaningful way without' that presence 'being physical in the traditional sense of the term.' A virtual showroom can show far more inventory, in far more detail, and with greater opportunities for consumer and seller interaction than might be possible for local stores.") (internal citations omitted); *see also* id. at 2096-99.

[53] In addition to the analysis presented herein, the Court accepts each aspect of SEVEN's opposition to the Motion in support of this Order's conclusion. (Dkt. Nos. 141, 154).

Akamai Techs., Inc. v. Limelight Networks, Inc.

United States Court of Appeals for the Federal Circuit

August 13, 2015, Decided

2009-1372, 2009-1380, 2009-1416, 2009-1417

Reporter
797 F.3d 1020 *; 2015 U.S. App. LEXIS 14175 **; 116 U.S.P.Q.2D (BNA) 1344 ***

AKAMAI TECHNOLOGIES, INC., THE MASSACHUSETTS INSTITUTE OF TECHNOLOGY, Plaintiffs-Appellants v. LIMELIGHT NETWORKS, INC., Defendant-Cross-Appellant

Subsequent History: Later proceeding at, Remanded by *V Limelight Networks, 805 F.3d 1368, 2015 U.S. App. LEXIS 19848 (Fed. Cir., Nov. 16, 2015)*

Prior History: [1]** Appeals from the United States District Court for the District of Massachusetts in Nos. 06-CV-11585, 06-CV-11109, Judge Rya W. Zobel.

Akamai Techs., Inc. v. Limelight Networks, Inc., 786 F.3d 899, 2015 U.S. App. LEXIS 7856 (Fed. Cir., 2015)
Akamai Tech., Inc. v. Limelight Networks, 494 F. Supp. 2d 34, 2007 U.S. Dist. LEXIS 47598 (D. Mass., 2007)

Core Terms

customers', infringement, steps, patent, tagging, substantial evidence, network, delivery, entity, serving, vicarious liability, alleged infringer, joint enterprise

Case Summary

Overview
HOLDINGS: [1]-Direct patent infringement by divided infringement under *35 U.S.C.S. § 271(a)* is not limited solely to principal-agent relationships, contractual arrangements, or joint enterprises, and a court considers whether all method steps can be attributed to a single entity; [2]-A provider of Internet services was properly found to have infringed a patent claiming methods for delivering content over the Internet, even though the provider's customers performed the content tagging and serving method steps, since the provider conditioned use of its network to the customers' performance of tagging and serving steps and thus directed or controlled the customers' infringing activities.

Outcome
Judgment of non-infringement reversed.

LexisNexis® Headnotes

Patent Law > Infringement Actions > Infringing Acts > General Overview

HN1[] **Infringement Actions, Infringing Acts**

Direct patent infringement under *35 U.S.C.S. § 271(a)* occurs where all steps of a claimed method are performed by or attributable to a single entity. Where more than one actor is involved in practicing the steps, a court must determine whether the acts of one are attributable to the other such that a single entity is responsible for the infringement. The court will hold an entity responsible for others' performance of method steps in two sets of circumstances: (1) where that entity directs or controls others' performance; and (2) where the actors form a joint enterprise.

Patent Law > Infringement Actions > Infringing Acts > General Overview

Patent Law > Jurisdiction & Review > Standards of Review > Substantial Evidence

HN2[] **Infringement Actions, Infringing Acts**

To determine if a single entity directs or controls the acts of another for purposes of patent infringement, a court considers general principles of vicarious liability. An actor is liable for patent infringement under *35*

U.S.C.S. § 271(a) if it acts through an agent (applying traditional agency principles) or contracts with another to perform one or more steps of a claimed method. Liability under *§ 271(a)* can also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance. In those instances, the third party's actions are attributed to the alleged infringer such that the alleged infringer becomes the single actor chargeable with direct infringement. Whether a single actor directed or controlled the acts of one or more third parties is a question of fact, reviewable on appeal for substantial evidence, when tried to a jury.

Business & Corporate Law > Joint Ventures > Formation

Patent Law > Infringement Actions > Infringing Acts > General Overview

Patent Law > Jurisdiction & Review > Standards of Review > Substantial Evidence

HN3 **Joint Ventures, Formation**

For purposes of patent infringement, where two or more actors form a joint enterprise, all can be charged with the acts of the other, rendering each liable for the patent steps performed by the other as if each is a single actor. A joint enterprise requires proof of four elements: (1) an agreement, express or implied, among the members of the group; (2) a common purpose to be carried out by the group; (3) a community of pecuniary interest in that purpose, among the members; and (4) an equal right to a voice in the direction of the enterprise, which gives an equal right of control. Whether actors entered into a joint enterprise is a question of fact, reviewable on appeal for substantial evidence.

Patent Law > Infringement Actions > Infringing Acts > General Overview

HN4 **Infringement Actions, Infringing Acts**

35 U.S.C.S. § 271(a) is not limited solely to principal-agent relationships, contractual arrangements, and joint enterprise. Rather, to determine direct patent infringement, a court considers whether all method steps can be attributed to a single entity.

Counsel: SETH P. WAXMAN, Wilmer Cutler Pickering Hale and Dorr LLP, Washington, DC, argued for plaintiffs-appellants. Also represented by THOMAS G. SAUNDERS, THOMAS G. SPRANKLING; MARK C. FLEMING, ERIC F. FLETCHER, LAUREN B. FLETCHER, BROOK HOPKINS, Boston, MA; DAVID H. JUDSON, Law Offices of David H. Judson, Dallas, TX; DONALD R. DUNNER, ELIZABETH D. FERRILL, Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, Washington, DC; JENNIFER S. SWAN, Palo Alto, CA; ROBERT S. FRANK, JR., G. MARK EDGARTON, CARLOS PEREZ-ALBUERNE, Choate, Hall & Stewart, LLP, Boston, MA.

AARON M. PANNER, Kellogg, Huber, Hansen, Todd, Evans & Figel, P.L.L.C., Washington, DC, argued for defendant-cross-appellant. Also represented by JOHN CHRISTOPHER ROZENDAAL, MICHAEL E. JOFFRE; MICHAEL W. DE VRIES, ALLISON W. BUCHNER, Kirkland & Ellis LLP, Los Angeles, CA; YOUNG JIN PARK, New York, NY; DION D. MESSER, Limelight Networks, Inc., Tempe, AZ.

JEFFREY I.D. LEWIS, Fried, Frank, Harris, Shriver & Jacobson LLP, New York, NY, for amicus curiae **[**2]** American Intellectual Property Law Association. Also represented by KRISTIN M. WHIDBY, Washington, DC; LISA K. JORGENSON, American Intellectual Property Law Association, Arlington, VA.

SCOTT A.M. CHAMBERS, Porzio, Bromberg & Newman, P.C., Washington, DC, for amicus curiae Biotechnology Industry Organization. Also represented by CAROLINE COOK MAXWELL; HANSJORG SAUER, Biotechnology Industry Organization, Washington, DC.

CHARLES R. MACEDO, Amster Rothstein & Ebenstein LLP, New York, NY, for amicus curiae Broadband iTV, Inc. Also represented by JESSICA CAPASSO.

PAUL H. BERGHOFF, McDonnell, Boehnen, Hulbert & Berghoff, LLP, Chicago, IL, for amicus curiae Intellectual Property Owners Association. Also represented by PHILIP S. JOHNSON, Johnson & Johnson, New Brunswick, NJ; KEVIN H. RHODES, 3M Innovative Properties Co., St. Paul, MN; HERBERT C. WAMSLEY, Intellectual Property Owners Association, Washington, DC.

CARTER G. PHILLIPS, Sidley Austin LLP, Washington, DC, for amicus curiae Pharmaceutical Research and Manufacturers of America. Also represented by JEFFREY P. KUSHAN, RYAN C. MORRIS; DAVID E. KORN, Pharmaceutical Research and Manufacturers **[**3]** of America, Washington, DC; DAVID R. MARSH, LISA A. ADELSON, Arnold & Porter,

LLP, Washington, DC; ROBERT P. TAYLOR, MONTY AGARWAL, San Francisco, CA.

DEMETRIUS TENNELL LOCKETT, Townsend & Lockett, LLC, Atlanta, GA, for amici curiae Nokia Technologies Oy and Nokia USA Inc.

DONALD R. WARE, Foley Hoag LLP, Boston, MA, for amicus curiae The Coalition for 21st Century Medicine. Also represented by MARCO J. QUINA, SARAH S. BURG.

Judges: Before PROST, Chief Judge, NEWMAN, LOURIE, LINN, DYK, MOORE, O'MALLEY, REYNA, WALLACH, and HUGHES, Circuit Judges.*

Opinion

[*1345] [*1022]** PER CURIAM.

This case was returned to us by the United States Supreme Court, noting "the possibility that [we] erred by too narrowly circumscribing the scope of *§ 271(a)*" and suggesting that we "will have the opportunity to revisit the *§ 271(a)* question . . . ." *Limelight Networks, Inc. v. Akamai Techs., Inc., 134 S. Ct. 2111, 2119, 2120, 189 L. Ed. 2d 52 (2014)*. We hereby avail ourselves of that opportunity.

Sitting en banc, we unanimously set forth the law of divided infringement under *35 U.S.C. § 271(a)*. We conclude that, in this case, substantial evidence supports the jury's finding that Limelight Networks, Inc. ("Limelight") directly infringes U.S. Patent 6,108,703 (the "'703 patent") under *§ 271(a)*. We therefore reverse the district court's grant of judgment of **[**4]** noninfringement as a matter of law.

I. DIVIDED INFRINGEMENT

HN1[] Direct infringement under *§ 271(a)* occurs where all steps of a claimed method are performed by or attributable to a single entity. *See BMC Res., Inc. v. Paymentech, L.P., 498 F.3d 1373, 1379-81 (Fed. Cir. 2007)*. Where more than one actor is involved in practicing the steps, a court must determine whether the acts of one are attributable to the other such that a single entity is responsible **[***1346]** for the infringement. We will hold an entity responsible for others' performance of method steps in two sets of circumstances: (1) where that entity directs or controls others' performance, and (2) where the actors form a joint enterprise.[1]

HN2[] To determine if a single entity directs or controls the acts of another, we continue to consider general principles of vicarious liability.[2] *See BMC, 498 F.3d at **[*1023]** 1379*. In the past, we have held that an actor is liable for infringement under *§ 271(a)* if it acts through an agent (applying traditional agency principles) or contracts with another to perform one or more steps of a claimed method. *See BMC, 498 F.3d at 1380-81*. We conclude, on the facts of this case, that liability under *§ 271(a)* can **[**5]** also be found when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance. *Cf. Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930, 125 S. Ct. 2764, 162 L. Ed. 2d 781 (2005)* (stating that an actor "infringes vicariously by profiting from direct infringement" if that actor has the right and ability to stop or limit the infringement).In those instances, the third party's actions are attributed to the alleged infringer such that the alleged infringer becomes the single actor chargeable with direct infringement. Whether a single actor directed or controlled the acts of one or more third parties is a question of fact, reviewable on appeal for substantial evidence, when tried to a jury.

HN3[] Alternatively, where two or more actors form a joint enterprise, all can be charged with the acts of the other, rendering each liable for the steps performed by the other as if each is a single actor. *See Restatement (Second) of Torts § 491 cmt. b* ("The law . . . considers that each is the agent or servant of the others, and that

---

* Circuit Judges Taranto, Chen, and Stoll did not participate.

[1] To the extent that our decision in *Golden Hour Data Systems, Inc. v. emsCharts, Inc., 614 F.3d 1367 (Fed. Cir. 2010)* is inconsistent with this conclusion, that aspect of *Golden Hour* is overruled.

[2] We note that previous cases' use of the term "vicarious liability" is a misnomer. *Restatement (Third) of Torts: Apportionment of Liability § 13* (2000). In the context of joint patent infringement, an alleged infringer is not liable for a third party's commission of infringement—rather, an alleged infringer is responsible for method steps performed by a third party. Accordingly, we recognize that vicarious liability is not a perfect analog. Nevertheless, as both vicarious liability and joint patent infringement discern **[**6]** when the activities of one entity are attributable to another, we derive our direction or control standard from vicarious liability law. *See BMC, 498 F.3d at 1379*.

the act of any one within the scope of the enterprise is to be charged vicariously against the rest."). A joint enterprise requires proof of four elements:

> (1) an agreement, express or implied, among the members of the group;
> (2) a common purpose to be carried out by the group;
> (3) a community of pecuniary interest in that purpose, among the members; and
> (4) an equal right to a voice in the direction of the enterprise, which gives an equal right of control.

Id. *§ 491 cmt. c.* As with direction or control, whether actors entered into a joint enterprise is a question of fact, reviewable on appeal for substantial evidence. *Id.* ("Whether these elements exist is frequently a question for the jury, under proper direction from the court.").

We believe these approaches to be most consistent **[**7]** with the text of *§ 271(a)*, the statutory context in which it appears, the legislative purpose behind the Patent Act, and our past case law. ***HN4***[↑] *Section 271(a)* is not limited solely to principal-agent relationships, contractual arrangements, and joint enterprise, as the vacated panel decision held.[3] Rather, to determine direct infringement, we consider whether all method steps can be attributed to a single entity.

II. Application to the Facts of This Case

Today we outline the governing legal framework for direct infringement and address the facts presented by this case. In the future, other factual scenarios may arise which warrant attributing others' performance of method steps to a single actor. Going forward, principles of attribution are to be considered in the context of the particular facts presented.

The facts of this case need not be repeated in detail once again, but the following **[*1024]** constitutes the basic facts. In 2006, Akamai Technologies, Inc. ("Akamai") filed a patent infringement **[***1347]** action against Limelight alleging infringement of several patents, including the '703 patent, which claims methods for **[**8]** delivering content over the Internet. The case proceeded to trial, at which the parties agreed that Limelight's customers—not Limelight—perform the "tagging" and "serving" steps in the claimed methods. For example, as for claim 34 of the '703 patent, Limelight performs every step save the "tagging" step, in which Limelight's customers tag the content to be hosted and delivered by Limelight's content delivery network. After the close of evidence, the district judge instructed the jury that Limelight is responsible for its customers' performance of the tagging and serving method steps if Limelight directs or controls its customers' activities. The jury found that Limelight infringed claims 19, 20, 21, and 34 of the '703 patent. Following post-trial motions, the district court first denied Limelight's motion for judgment of noninfringement as a matter of law, ruling that Akamai had presented substantial evidence that Limelight directed or controlled its customers. After we decided *Muniauction, Inc. v. Thomson Corp., 532 F.3d 1318 (Fed. Cir. 2008)*, the district court granted Limelight's motion for reconsideration, holding as a matter of law that there could be no liability.

We reverse and reinstate the jury verdict. The jury heard substantial evidence from which it could find **[**9]** that Limelight directs or controls its customers' performance of each remaining method step, such that all steps of the method are attributable to Limelight. Specifically, Akamai presented substantial evidence demonstrating that Limelight conditions its customers' use of its content delivery network upon its customers' performance of the tagging and serving steps, and that Limelight establishes the manner or timing of its customers' performance. We review the evidence supporting "conditioning use of the content delivery network" and "establishing the manner or timing of performance" in turn.

First, the jury heard evidence that Limelight requires all of its customers to sign a standard contract. The contract delineates the steps customers must perform if they use the Limelight service. These steps include tagging and serving content. As to tagging, Limelight's form contract provides: "Customer shall be responsible for identifying via the then current [Limelight] process all [URLs] of the Customer Content to enable such Customer Content to be delivered by the [Limelight network]." J.A. 17807. In addition, the contract requires that Limelight's customers "provide [Limelight] with all cooperation **[**10]** and information reasonably necessary for [Limelight] to implement the [Content Delivery Service]." *Id.* As for the serving step, the form contract states that Limelight is not responsible for failures in its content delivery network caused by its customers' failure to serve content. *See id.* If a customer's server is down, Limelight's content delivery network need not perform. Thus, if Limelight's customers wish to use Limelight's product, they must

---

[3] To the extent our prior cases formed the predicate for the vacated panel decision, those decisions are also overruled.

tag and serve content. Accordingly, substantial evidence indicates that Limelight conditions customers' use of its content delivery network upon its customers' performance of the tagging and serving method steps.

Substantial evidence also supports finding that Limelight established the manner or timing of its customers' performance. Upon completing a deal with Limelight, Limelight sends its customer a welcome letter instructing the customer how to use Limelight's service. In particular, the **[*1025]** welcome letter tells the customer that a Technical Account Manager employed by Limelight will lead the implementation of Limelight's services. J.A. 17790. The welcome letter also contains a hostname assigned by Limelight that the customer "integrate[s] into [its] webpages." **[**11]** J.A. 17237; 17790. This integration process includes the tagging step. Moreover, Limelight provides step-by-step instructions to its customers telling them how to integrate Limelight's hostname into its webpages if the customer wants to act as the origin for content. J.A. 17220. If Limelight's customers do not follow these precise steps, Limelight's service will not be available. J.A. 587 at 121:22-122:22. Limelight's Installation Guidelines give Limelight customers further information on tagging content. J.A. 17791. Lastly, the jury heard evidence that Limelight's engineers continuously engage with customers' activities. Initially, Limelight's engineers assist with installation and perform quality assurance testing. J.A. 17790. The engineers remain available if the customer experiences any problems. J.A. 17235. In sum, Limelight's customers do not merely take Limelight's guidance and act independently on their own. Rather, Limelight establishes the manner and timing of its customers' **[***1348]** performance so that customers can only avail themselves of the service upon their performance of the method steps.

We conclude that the facts Akamai presented at trial constitute substantial evidence from **[**12]** which a jury could find that Limelight directed or controlled its customers' performance of each remaining method step. As such, substantial evidence supports the jury's verdict that all steps of the claimed methods were performed by or attributable to Limelight. Therefore, Limelight is liable for direct infringement.

III. CONCLUSION

At trial, Akamai presented substantial evidence from which a jury could find that Limelight directly infringed the '703 patent. Therefore, we reverse the district court's grant of judgment of noninfringement as a matter of law. Because issues in the original appeal and cross-appeal remain, we return the case to the panel for resolution of all residual issues consistent with this opinion.

End of Document

Eli Lilly & Co. v. Teva Parenteral Meds., Inc.

United States Court of Appeals for the Federal Circuit

January 12, 2017, Decided

2015-2067

Reporter
845 F.3d 1357 *; 2017 U.S. App. LEXIS 555 **; 121 U.S.P.Q.2D (BNA) 1277 ***; 2017 WL 117164

ELI LILLY AND COMPANY, Plaintiff-Appellee v. TEVA PARENTERAL MEDICINES, INC., APP PHARMACEUTICALS LLC, PLIVA HRVATSKA D.O.O., TEVA PHARMACEUTICALS USA, INC., BARR LABORATORIES, INC., Defendants-Appellants

Subsequent History: Related proceeding at *Eli Lilly & Co. v. Glenmark Generics Inc., 2017 U.S. Dist. LEXIS 128604 (S.D. Ind., Aug. 11, 2017)*

Prior History: [1]** Appeal from the United States District Court for the Southern District of Indiana in No. 1:10-cv-01376-TWPDKL, Judge Tanya Walton Pratt.

Eli Lilly & Co. v. Teva Parenteral Meds., Inc., 126 F. Supp. 3d 1037, 2015 U.S. Dist. LEXIS 112221 (S.D. Ind., Aug. 25, 2015)
Eli Lilly & Co. v. Teva Parenteral Meds., Inc., 2014 U.S. Dist. LEXIS 43885 (S.D. Ind., Mar. 31, 2014)
Eli Lilly & Co. v. Teva Parenteral Meds., Inc., 2012 U.S. Dist. LEXIS 85369 (S.D. Ind., June 20, 2012)

Disposition: AFFIRMED.

Core Terms

vitamin, pemetrexed, folic acid, infringement, patent, patients, skilled, district court, asserted claim, labeling, induce, pretreatment, toxicities, instructions, dose, cyanocobalamin, artisan, administering, prior art, references, invalid, steps, indefiniteness, ordinary person, supplementation, schedules, recites, Prescribing, acid, double patenting

Case Summary

Overview

HOLDINGS: [1]-The record supported the district court's judgment that pharmaceutical companies that proposed to manufacture a generic form of the chemotherapy drug pemetrexed disodium could not do so without inducing infringement of U.S. Patent No. 7,772,209 ("the '209 patent"), in violation of *35 U.S.C.S. § 271*, because the '209 patent protected a method for using pemetrexed that required patients to take specified doses of folic acid and vitamin B12 to avoid side effects that could occur, and that method was required to use the generic drugs the pharmaceutical companies proposed to manufacture; [2]-The '209 patent was not invalid for indefiniteness under former *35 U.S.C.S. § 112, para. 2* (replaced 2012) because it used the term "vitamin B12" but did not define that term.

Outcome
The court of appeals affirmed the district court's judgment.

LexisNexis® Headnotes

Business & Corporate Compliance > ... > Infringement Actions > Infringing Acts > Indirect Infringement

Evidence > Burdens of Proof > Preponderance of Evidence

Patent Law > Jurisdiction & Review > Standards of Review > Clearly Erroneous Review

HN1[] **Infringing Acts, Indirect Infringement**

Pursuant to *35 U.S.C.S. § 271(b)*, whoever actively induces infringement of a patent shall be liable as an infringer. Importantly, liability for induced infringement under *§ 271(b)* must be predicated on direct infringement. A patentee must also show that the

alleged infringer possessed the requisite intent to induce infringement, which requires that the alleged infringer knew or should have known his actions would induce actual infringements. A patentee seeking relief under *§ 271(e)(2)* bears the burden of proving infringement by a preponderance of the evidence. Infringement is a question of fact that, after a bench trial, the United States Court of Appeals for the Federal Circuit reviews for clear error. Reversal for clear error is appropriate only when the court of appeals is left with a definite and firm conviction that a district court was in error.

Patent Law > Infringement Actions > Infringing Acts > Intent & Knowledge

Patent Law > ... > Claims > Claim Language > Product by Process

Patent Law > Subject Matter > Utility Patents > Process Patents

HN2 **Infringing Acts, Intent & Knowledge**

Where no single actor performs all steps of a method claim, direct infringement only occurs if the acts of one are attributable to the other, such that a single entity is responsible for the infringement. The performance of method steps is attributable to a single entity in two types of circumstances: when that entity directs or controls others' performance, or when the actors form a joint enterprise.

Business & Corporate Compliance > ... > Infringement Actions > Infringing Acts > Indirect Infringement

HN3 **Infringing Acts, Indirect Infringement**

In its 2015 decision in Akamai Technologies, Inc. v. Limelight Networks, Inc., the United States Court of Appeals for the Federal Circuit held that directing or controlling others' performance includes circumstances in which an actor: (1) conditions participation in an activity or receipt of a benefit upon others' performance of one or more steps of a patented method; and (2) establishes the manner or timing of that performance. In addition to this two-prong test, the Federal Circuit observed that in the future, factual scenarios may arise which warrant attributing others' performance of method steps to a single actor. Going forward, principles of attribution are to be considered in the context of the particular facts presented.

Business & Corporate Compliance > ... > Infringement Actions > Infringing Acts > Indirect Infringement

HN4 **Infringing Acts, Indirect Infringement**

The United States Court of Appeals for the Federal Circuit rejects the argument that an actor can only condition the performance of a step by imposing a legal obligation to do so, by interposing that step as an unavoidable technological prerequisite to participation, or both. In its 2015 decision in Akamai Technologies, Inc. v. Limelight Networks, Inc., the Federal Circuit found "conditioning" based on evidence that a defendant required all of its customers to sign a standard contract delineating the steps that customers had to perform to use the defendant's service. But the court did not limit "conditioning" to legal obligations or technological prerequisites. The court cautioned that principles of attribution are to be considered in the context of the particular facts presented, and expressly held that *35 U.S.C.S. § 271(a)* infringement is not limited solely to principal-agent relationships, contractual arrangements, and a joint enterprise.

Business & Corporate Compliance > ... > Infringement Actions > Infringing Acts > Indirect Infringement

Patent Law > Infringement Actions > Infringing Acts > Intent & Knowledge

HN5 **Infringing Acts, Indirect Infringement**

The mere existence of direct infringement by physicians, while necessary to find liability for induced infringement, is not sufficient for inducement. To show inducement, a patent holder carries the burden of proving specific intent and action to induce infringement. Mere knowledge of the acts alleged to constitute infringement is not sufficient.

Business & Corporate Compliance > ... > Infringement Actions > Infringing Acts > Indirect Infringement

Patent Law > Infringement Actions > Infringing Acts > Intent & Knowledge

HN6 **Infringing Acts, Indirect Infringement**

The intent for inducement must be with respect to the actions of an underlying direct infringer. The United States Court of Appeals for the Federal Circuit has not required evidence regarding the general prevalence of the induced activity. When an alleged inducement relies on a drug label's instructions, the question is not just whether those instructions describe the infringing mode, but whether the instructions teach an infringing use such that the Federal Circuit is willing to infer from those instructions an affirmative intent to infringe the patent. A label must encourage, recommend, or promote infringement. For purposes of inducement, it is irrelevant that some users may ignore the warnings in a proposed label. Depending on the clarity of the instructions, the decision to continue seeking FDA approval of those instructions may be sufficient evidence of specific intent to induce infringement. The Federal Circuit held in AstraZeneca LP v. Apotex, Inc. that a label that instructed users to follow the instructions in an infringing manner was sufficient even though some users would not follow the instructions. That was true even though the product in question had substantial noninfringing uses. Conversely, "vague" instructions that require one to look outside a label to understand the alleged implicit encouragement do not, without more, induce infringement.

Business & Corporate Compliance > ... > Infringement Actions > Infringing Acts > Indirect Infringement

HN7 **Infringing Acts, Indirect Infringement**

Where product labeling already encourages infringement of asserted claims, a physician's decision to give patients even more specific guidance is irrelevant to the question of inducement.

Patent Law > ... > Specifications > Definiteness > Precision Standards

HN8 **Definiteness, Precision Standards**

Pursuant to former 35 U.S.C.S. § 112, para. 2 (replaced 2012), a patent's specification must conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Patent Law > Jurisdiction & Review > Standards of Review > De Novo Review

Patent Law > ... > Specifications > Definiteness > Precision Standards

Patent Law > ... > Specifications > Definiteness > Fact & Law Issues

HN9 **Standards of Review, De Novo Review**

In Nautilus, Inc. v. Biosig Instruments, Inc., the United States Supreme Court rejected the United States Court of Appeals for the Federal Circuit's "not amenable to construction or insolubly ambiguous" standard for indefiniteness and articulated, instead, that a patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention. Indefiniteness is a question of law that the Federal Circuit reviews de novo, and the Federal Circuit has reiterated post-Nautilus that general principles of claim construction apply to the question of indefiniteness. The Federal Circuit reviews subsidiary factual determinations made by a district court based on extrinsic evidence for clear error.

Patent Law > ... > Specifications > Definiteness > Fact & Law Issues

HN10 **Definiteness, Fact & Law Issues**

Understandings that lie outside patent documents about the meaning of terms to one of skill in the art or the science or state of the knowledge of one of skill in the art are factual issues.

Patent Law > Infringement Actions > Claim Interpretation > Claim Differentiation

Patent Law > ... > Claims > Claim Language > Dependent Claims

HN11 **Claim Interpretation, Claim Differentiation**

The doctrine of claim differentiation presumes that dependent claims are of narrower scope than the independent claims from which they depend.

Patent Law > ... > Claims > Claim Language > Duplication & Multiplicity

HN12 **Claim Language, Duplication & Multiplicity**

Although the United States Court of Appeals for the Federal Circuit has in some instances interpreted claim terms to avoid redundancy, the rule is not inflexible.

Patent Law > Jurisdiction & Review > Standards of Review > Clearly Erroneous Review

Patent Law > Nonobviousness > Elements & Tests > Ordinary Skill Standard

Patent Law > Nonobviousness > Elements & Tests > Prior Art

Patent Law > Nonobviousness > Evidence > Fact & Law Issues

Patent Law > Jurisdiction & Review > Standards of Review > De Novo Review

HN13 **Standards of Review, Clearly Erroneous Review**

To prevail on obviousness, an alleged infringer must prove by clear and convincing evidence that a skilled artisan would have been motivated to combine the teachings of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so. Obviousness is a question of law based on underlying facts, and on appeal from a bench trial, the United States Court of Appeals for the Federal Circuit reviews the district court's conclusions of law de novo and findings of fact for clear error.

Patent Law > Double Patenting

HN14 **Patent Law, Double Patenting**

The judicially-created doctrine of "obviousness-type double patenting" is intended to prevent the extension of the term of a patent by prohibiting the issuance of the claims in a second patent that are not patentably distinct from claims of the first patent. After determining the differences in the claims of the earlier and later patents, a court must determine if the alleged infringer has proven by clear and convincing evidence that the claims are not patentably distinct. A later patent claim is not patentably distinct from an earlier claim if the later claim is obvious over, or anticipated by, the earlier claim. Even where a patent is found invalid for obviousness-type double patenting, though, a patentee may file a terminal disclaimer. Obviousness-type double patenting is a question of law based on underlying facts, so on appeal from a bench trial, the United States Court of Appeals for the Federal Circuit reviews a district court's conclusions of law de novo and findings of fact for clear error.

Counsel: ADAM LAWRENCE PERLMAN, Williams & Connolly LLP, Washington, DC, argued for plaintiff-appellee. Also represented by DOV PHILIP GROSSMAN, BRUCE GENDERSON, DAVID M. KRINSKY, ALLISON JONES RUSHING, ELLEN E. OBERWETTER.

WILLIAM M. JAY, Goodwin Procter LLP, Washington, DC, argued for defendants-appellants. Also represented by DARYL L. WIESEN, ELAINE BLAIS, EMILY L. RAPALINO, HENRY C. DINGER, Boston, MA; BRIAN JOSEPH PREW, MICHAEL B. COTTLER, NATASHA ELISE DAUGHTREY, New York, NY.

CHRISTINA JORDAN MCCULLOUGH, Perkins Coie, LLP, Seattle, WA, for amicus curiae Generic Pharmaceutical Association. Also represented by SHANNON BLOODWORTH, Washington, DC.

KEVIN SCOTT PRUSSIA, Wilmer Cutler Pickering Hale and Dorr LLP, Boston, MA, for amicus curiae Pharmaceutical Research and Manufacturers of America. Also represented by SAMEER AHMED; JAMIE WISZ, Washington, DC.

DAVID S. FORMAN, Osha Liang LLP, Alexandria, VA, for amicus curiae Biotechnology Innovation Organization. Also represented by HANSJORG SAUER, Biotechnology Innovation Organization, Washington, DC.

Judges: Before **[**2]** PROST, Chief Judge, NEWMAN and DYK, Circuit Judges.

Opinion by: PROST

Opinion

[*1361] [*1279]** PROST, *Chief Judge*.

Eli Lilly & Co. ("Eli Lilly") is the owner of U.S. Patent No. 7,772,209 ("'209 patent"). It filed this consolidated Hatch-Waxman suit against Teva Parenteral Medicines, Inc.; APP Pharmaceuticals LLC; Pliva Hrvatska D.O.O.; Teva Pharmaceuticals USA, Inc.; and Barr Laboratories, Inc. (collectively, "Defendants") to prevent Defendants from launching a generic version of a chemotherapy drug with accompanying product literature that would allegedly infringe methods of treatment claimed by the '209 patent. The United States District Court for the Southern District of Indiana held two bench trials, one on infringement and one on invalidity. The district court found that no single actor performs all steps of the asserted claims because the actions of both physicians and patients are required. Nonetheless, under *Akamai Technologies, Inc. v. Limelight Networks, Inc. (Akamai V), 797 F.3d 1020, 1022 (Fed. Cir. 2015)* (en banc) (per curiam), *cert. denied*, *136 S. Ct. 1661, 194 L. Ed. 2d 767 (2016)*, the court found direct infringement attributable to physicians and held Defendants liable for inducing that infringement. The court also determined that the asserted claims were not invalid for, inter alia, indefiniteness, obviousness, or obviousness-type double patenting.

For the reasons below, we affirm.

[*1280]** BACKGROUND

The '209 patent **[**3]** , which issued in 2010, relates to methods of administering the chemotherapy drug pemetrexed disodium ("pemetrexed") after pretreatment with two common vitamins—folic acid and vitamin B12. Pemetrexed is an antifolate that kills cancer cells by inhibiting the function **[*1362]** of folates, a class of nutrients necessary for cell reproduction. The purpose of the dual vitamin pretreatments is to reduce the toxicity of pemetrexed in patients. Eli Lilly markets pemetrexed under the brand name ALIMTA®, and the drug is used to treat certain types of lung cancer and mesothelioma.

Around 2008-2009, Defendants notified Eli Lilly that they had submitted Abbreviated New Drug Applications ("ANDAs") seeking approval by the Food and Drug Administration ("FDA") to market generic versions of ALIMTA®. After the '209 patent issued, Defendants sent Eli Lilly additional notices regarding their ANDAs, including notices that they had filed Paragraph IV certifications under *21 U.S.C. § 355(j)(2)(A)(vii)(IV)*, declaring that the '209 patent was invalid, unenforceable, or would not be infringed. Eli Lilly subsequently brought this consolidated action against Defendants for infringement under *35 U.S.C. § 271(e)(2)*. Specifically, Eli Lilly alleged that Defendants' generic drugs would be administered **[**4]** with folic acid and vitamin B12 pretreatments and, thus, result in infringement of the '209 patent. Defendants raised noninfringement and invalidity defenses.

Eli Lilly asserted claims 9, 10, 12, 14, 15, 18, 19, and 21 of the '209 patent at trial. Importantly, all of the asserted claims require patient pretreatment by "administering" or "administration of" folic acid. Claims 9 and 10 depend from claim 1, which recites:

> 1. A method of administering pemetrexed disodium to a patient in need thereof comprising *administering an effective amount of folic acid* and an effective amount of a methylmalonic acid lowering agent followed by administering an effective amount of pemetrexed disodium, wherein the methylmalonic acid lowering agent is selected from the group consisting of vitamin B12, hydroxycobalamin, cyano-10-chlorocobalamin, aquocobalamin perchlorate, aquo-10-cobalamin perchlorate, azidocobalamin, cobalamin, cyanocobalamin, or chlorocobalamin.

'209 patent col. 10 ll. 55-65 (emphasis added). The additional limitations of claims 9 and 10 restrict the dose of folic acid to particular ranges. *Id.* at col. 11 ll. 19-22.

Asserted claim 12 is independent and recites:

> 12. An improved method for administering pemetrexed disodium **[**5]** to a patient in need of chemotherapeutic treatment, wherein the improvement comprises:
>
> > a) *administration of between about 350 µg and about 1000 µg of folic acid* prior to the first administration of pemetrexed disodium;
> > b) administration of about 500 µg to about 1500 µg of vitamin B12, prior to the first administration of pemetrexed disodium; and
> > c) administration of pemetrexed disodium.

Id. at col. 11 l. 25-col. 12 l. 4 (emphasis added).

Asserted claims 14, 15, 18, 19, and 21 depend from claim 12 and further limit the dose, schedule, or route of folic acid or vitamin B12 administration. *Id.* at col. 12 ll. 7-11, col. 12 ll. 16-20, col. 12 ll. 24-27.

The parties agree for purposes of this appeal that no single actor performs all steps of the asserted claims; rather, the steps are divided between physicians and patients. Though physicians administer vitamin B12 and pemetrexed, patients self-administer folic acid with guidance from physicians. Eli Lilly's theory of infringement therefore requires establishing liability for divided infringement—an area of **[*1363]** law that this court was actively reconsidering during the pendency of this case.

In June 2013, Defendants conditionally conceded induced infringement **[**6]** **[*1364]** under then-current law set forth in *Akamai Technologies, Inc. v. Limelight Networks, Inc. (Akamai II), 692 F.3d 1301 (Fed. Cir. 2012)* (en banc) (per curiam), *rev'd*, *134 S. Ct. 2111, 189 L. Ed. 2d 52 (2014)*.[1] At the time, the *Akamai II* decision was the subject of a petition to the Supreme Court for a writ of certiorari. The parties' stipulation included a provision reserving Defendants' right to litigate infringement if the Supreme Court reversed or vacated *Akamai II*.

Eli Lilly and Defendants proceeded with a bench trial on invalidity, after which the district court held that the asserted claims were **[***1281]** not invalid for, inter alia, obviousness or obviousness-type double patenting. The court had also previously rejected Defendants' contention that the asserted claims were invalid for indefiniteness of the term "vitamin B12." Defendants filed an appeal on invalidity, which was docketed in this court as Case No. 14-1455. While that appeal was pending, the Supreme Court reversed *Akamai II*, holding that liability for inducement cannot be found without direct infringement, and remanding for this court to possibly reconsider the standards for direct infringement. *Limelight Networks, Inc. v. Akamai Techs., Inc. (Akamai III), 134 S. Ct. 2111, 189 L. Ed. 2d 52 (2014)*. In view of that development, the parties in this case filed a joint motion to remand the matter to the district court for the limited purpose of litigating infringement. **[**7]** We granted the motion.

The district court held a second bench trial in May 2015 and concluded in a decision issued on August 25, 2015 that Defendants would induce infringement of the '209 patent. As explained in further detail below, the court applied our intervening *Akamai V* decision, which had broadened the circumstances in which others' acts may be attributed to a single actor to support direct-infringement liability in cases of divided infringement.[2] *See Akamai V, 797 F.3d at 1022*. The court accordingly entered final judgment against Defendants, barring them from launching their generic products before the expiration of the '209 patent.

Defendants timely appealed. We have jurisdiction under *28 U.S.C. § 1295(a)(1)*.

DISCUSSION

Defendants appeal the district court's finding of induced infringement, as well as the court's decision that the asserted claims are not invalid for indefiniteness, obviousness, or obviousness-type double patenting. We will address each of these issues in turn.

I

HN1[↑] Pursuant to *35 U.S.C. § 271(b)*, "[w]hoever actively induces infringement of a patent shall be liable as an infringer."[3] Importantly, liability for induced infringement under *§ 271(b)* "must be predicated on direct infringement." *Akamai III, 134 S. Ct. at 2117*. The patentee must also show that the alleged infringer possessed **[**8]** the requisite intent to induce infringement, which we have held requires that the alleged infringer "knew or should have known his actions would induce actual infringements." *DSU Med. Corp. v. JMS Co., 471 F.3d 1293, 1304 (Fed. Cir. 2006)* (en banc in relevant part) (internal quotation marks omitted). A patentee seeking relief under *§ 271(e)(2)* bears the burden of proving infringement by a preponderance of the evidence. *Warner-Lambert Co. v. Apotex Corp., 316 F.3d 1348, 1366 (Fed. Cir. 2003)*.

---

[1] *Akamai II* held that "induced infringement can be found even if there is no single party who would be liable for direct infringement." *692 F.3d at 1317-18*.

[2] Following remand from the Supreme Court, a panel of this court initially found that the accused infringer in *Akamai* was not liable for direct infringement, *Akamai Techs., Inc. v. Limelight Networks, Inc. (Akamai IV), 786 F.3d 899 (Fed. Cir. 2015)*, as had the first panel in the case, *Akamai Techs., Inc. v. Limelight Networks, Inc. (Akamai I), 629 F.3d 1311 (Fed. Cir. 2010)*. We later vacated *Akamai IV* and took the case en banc, which resulted in the *Akamai V* decision.

[3] ***Section 271*** was not amended by the Leahy-Smith America Invents Act ("AIA"), ***Pub. L. No. 112-29, 125 Stat. 284 (2011)***.

"Infringement is a question of fact that, after a bench trial, we review for clear error." *Alza Corp. v. Mylan Labs, Inc., 464 F.3d 1286, 1289 (Fed. Cir. 2006)*. Reversal for clear error is appropriate "only when this court is left with a definite and firm conviction that the district court was in error." *Id.*

The district court relied in part on Defendants' proposed product labeling as evidence of infringement. For purposes of this case, the parties have agreed that Defendants' product labeling would be materially the same as the ALIMTA® product labeling, which consists of two documents: the Physician Prescribing Information and the Patient Information. Both documents include instructions regarding the administration of folic acid—the step that the district court found would be performed by patients but attributable to physicians. For example, the Physician Prescribing Information provides, among other things: **[**9]**

> "Instruct patients to initiate folic acid 400 [µg] to 1000 [µg] orally once daily beginning 7 days before the first dose of [pemetrexed] . . . ." J.A. 11256.
>
> "Instruct patients on the need for folic acid and vitamin B_{12} supplementation to reduce treatment-related hematologic and gastrointestinal toxicity . . . ." J.A. 11278.

The Patient Information includes similar information:

> **[***1282]** "To lower your chances of side effects of [pemetrexed], you must also take folic acid . . . prior to and during your treatment with [pemetrexed]." J.A. 11253 (emphasis omitted).
>
> "It is very important to take folic acid and vitamin B12 during your treatment with [pemetrexed] to lower your chances of harmful side effects. You must start taking 400-1000 micrograms of folic acid every day for at least 5 days out of the 7 days before your first dose of [pemetrexed]. . . ." *Id.* (emphasis omitted).

A

HN2[↑] Where, as here, no single actor performs all steps of a method claim, direct infringement only occurs if "the acts of one are attributable to the other such that a single entity is responsible for the infringement." *Akamai V, 797 F.3d at 1022*. The performance of method steps is attributable to a single entity in two types of circumstances: when that entity **[**10]** "directs or controls" others' performance, or when the actors "form a joint enterprise." *Id.* Eli Lilly did not pursue a joint enterprise theory, so the question of direct infringement before us is whether physicians direct or control their patients' administration of folic acid.[4]

HN3[↑] **[*1365]** In *Akamai V*, we held that directing or controlling others' performance includes circumstances in which an actor: (1) "*conditions* participation in an activity or receipt of a benefit" upon others' performance of one or more steps of a patented method, and (2) "*establishes the manner or timing* of that performance." *Id. at 1023* (emphases added). In addition to this two-prong test, we observed that, "[i]n the future, other factual scenarios may arise which warrant attributing others' performance of method steps to a single actor. Going forward, principles of attribution are to be considered in the context of the particular facts presented." *Id.*

Here, the district court decided that "the factual circumstances [we]re sufficiently analogous to those in *Akamai* [*V*] to support a finding of direct infringement by physicians." *Eli Lilly & Co. v. Teva Parenteral Meds., Inc. (Eli Lilly III), 126 F. Supp. 3d 1037, 1041 (S.D. Ind. 2015)*. The court observed initially that taking folic acid in the manner recited by the asserted claims is a "critical" **[**11]** and "necessary" step to "reduc[e] . . . potentially life-threatening toxicities caused by pemetrexed," i.e., to "receive the benefit of the patented method." *Id. at 1042*. Regarding the first *Akamai V* prong, the court found, based on the product labeling, that "taking folic acid in the manner specified is a condition of the patient's participation in pemetrexed treatment." *Id.* Regarding the second prong, the court found that physicians would "prescrib[e] an exact dose of folic acid and direct[] that it be ingested daily." *Id. at 1043*. The court therefore held that, under *Akamai V*, the performance of all steps of the asserted claims would be attributable to physicians.

1

With respect to the first prong—conditioning participation in an activity or receipt of a benefit upon performance of one or more method steps—Defendants argue at the outset that the district court did not make a relevant finding because it misidentified the benefit that

---

[4] Before the district court, Eli Lilly also asserted theories of direct infringement that did not rely on showing physicians' direction or control of patient action, arguing that: (1) as a matter of claim construction, physicians "administer" folic acid; and (2) under the doctrine of equivalents, physicians' actions are equivalent to putting folic acid into patients' bodies. The district court did not reach those issues. Although Eli Lilly asks us to reach them in the alternative, we need not do so in light of our decision to affirm the district court under *Akamai V.*

would be conditioned as the "benefit of the patented method, i.e., a reduction of potentially life-threatening toxicities caused by pemetrexed." Appellants' Opening Br. 21-22. We agree that a reduction in toxicities is not a benefit that physicians can condition (as it follows from folic acid **[**12]** pretreatment) and that the relevant benefit that may be conditioned on folic acid administration is pemetrexed treatment. But the court's discussion of reducing pemetrexed toxicities in relation to its direction-or-control analysis was not erroneous. A reduction in pemetrexed toxicities is relevant only if pemetrexed treatment is administered, and it provides a reason why physicians would condition the receipt of pemetrexed treatment on folic acid administration. The court recognized this relationship and correctly identified pemetrexed treatment as the benefit to be conditioned: "What is relevant is whether the physician sufficiently directs or controls the acts of the patients in such a manner as to condition participation in an activity or receipt of a benefit—*in this case, treatment with pemetrexed* in the manner that reduces toxicities—upon the performance **[***1283]** of a step of the patented method and establishes the manner and timing of the performance." *Eli Lilly III, 126 F. Supp. 3d at 1042* (emphasis added); *see also id.* ("[T]aking folic acid in the manner specified is a condition of the patient's participation in *pemetrexed treatment*." (emphasis added)).

[*1366] The district court's finding that physicians "condition" pemetrexed treatment **[**13]** on the administration of folic acid is supported by the record evidence. The Physician Prescribing Information, which is "directed to the physician," J.A. 2181, explains that folic acid is a "[r]equirement for [p]remedication" in order "to reduce the severity of hematologic and gastrointestinal toxicity of [pemetrexed]." J.A. 11258. Consistent with the importance of folic acid pre-treatment, the product labeling repeatedly states that physicians should "[i]nstruct patients" to take folic acid and includes information about folic acid dosage ranges and schedules. J.A. 11256; *see also* J.A. 11255, 11278. The Patient Information also informs patients that physicians may withhold pemetrexed treatment: "You will have regular blood tests before and during your treatment with [pemetrexed]. *Your doctor may adjust your dose of [pemetrexed] or delay treatment* based on the results of your blood test and on your general condition." J.A. 11253 (emphasis added).

Furthermore, Eli Lilly's expert, Dr. Chabner, testified that it is "the physician's responsibility to initiate the supplementation" of folic acid. J.A. 2181. He explained that the product labeling shows that taking folic acid is "an absolute requirement" before pemetrexed treatment **[**14]** because "it wouldn't be safe to take the drug without the vitamin supplementation. . . . [I]t must be done this way." J.A. 2192; *see also* J.A. 2195 ("[I]t's an absolute requirement."), 2246 ("I think it's that important."). He further testified that if a physician realizes that a patient did not follow his or her instructions to take folic acid, then the "doctor will not give the pemetrexed." J.A. 2218. Even Defendants' expert, Dr. Schulz, acknowledged that it is "standard practice"—both his personally and physicians' generally—that a patient "must have taken their required folic acid in order to have the pemetrexed administered." J.A. 2329-40; *see also* J.A. 2304 ("I would withhold the pemetrexed therapy until [the patient] had initiated or resumed their folic acid treatment . . . [s]o as to avoid the toxicities associated with pemetrexed without vitamin replacement."). Dr. Schulz agreed that he was "not aware of any reputable institution or doctor . . . who, when they think the patient hasn't taken the required folic acid" would go ahead and administer pemetrexed. J.A. 2330-31.

The record is thus replete with evidence that physicians delineate the step of folic acid administration that patients **[**15]** must perform if they wish to receive pemetrexed treatment.

Defendants argue that mere guidance or instruction is insufficient to show "conditioning" under *Akamai V.* But the evidence regarding the critical nature of folic acid pretreatment and physicians' practices support a finding that physicians cross the line from merely guiding or instructing patients to take folic acid to conditioning pemetrexed treatment on their administration of folic acid. If a patient does not take folic acid as instructed, a physician, in his or her discretion, need not provide pemetrexed treatment based on the patient's failure to perform the step of folic acid administration. Defendants also complain that there is no evidence that physicians go further to "verify compliance" with their instructions or to "threaten" denial of pemetrexed treatment. Appellants' Opening Br. 22. Conditioning, however, does not necessarily require double-checking another's performance or making threats.

HN4[↑] We also reject Defendants' argument that an actor can only condition the performance of a step "by imposing a legal obligation to do so, by interposing that **[*1367]** step as an unavoidable technological prerequisite to participation, or, **[**16]** as in [*Akamai V*], both." *Id.* In *Akamai V*, we found "conditioning" based on

evidence that the defendant required all of its customers to sign a standard contract delineating the steps that customers had to perform to use the defendant's service. *797 F.3d at 1024*. But we did not limit "conditioning" to legal obligations or technological prerequisites.[5] We cautioned that "principles of attribution are to be considered in the context of the particular facts presented" and even expressly held that *§ 271(a)* infringement "is not limited solely to principal-agent relationships, contractual arrangements, and joint enterprise." *Id. at 1023*.

[*1284]** The product labeling, combined with the testimony discussed above, provide sufficient evidence that physicians condition pemetrexed treatment on folic acid pre-treatment.

2

With respect to the second prong—establishing the manner or timing of performance—Defendants argue that the product labeling "gives patients wide berth to select the dose . . . , the dosage form . . . , and the timing . . . of folic acid self-administration." Appellants' Opening Br. 23. Eli Lilly submits that expert testimony and product labeling demonstrate that "physicians prescribe or specify a dose of folic **[**17]** acid, specify that patients must ingest the folic acid daily during a particular span of days, and withhold pemetrexed if patients do not follow orders." Appellee's Br. 25. We agree with Eli Lilly.

The product labeling is again informative. For instance, the Physician Prescription Information instructs physicians not only to tell patients to take folic acid orally, but also to take "400 [µg] to 1000 [µg] [of folic acid] once daily beginning 7 days before the first dose of [pemetrexed]," accompanied with warnings about the consequences of non-compliance. J.A. 11256. That dosage range and schedule overlaps with all of the asserted claims' dosage ranges and schedules.[6] In addition, Dr. Chabner testified that "it's the doctor" who "decides how much [folic acid] the patient will take and when the patient takes it." J.A. 2197. In view of the record evidence, the court's finding that physicians establish the manner and timing of patients' folic acid intake is not clearly erroneous. Even if, as Defendants argue, patients are able to seek additional outside assistance regarding folic acid administration, such guidance is beyond what is required here to establish the manner or timing of performance **[**18]** and is therefore immaterial.

We therefore see no reversible error in the district court's finding that physicians condition patient participation in an activity **[*1368]** or receipt of a benefit (pemetrexed treatment) on folic acid administration and also establish the manner or timing of performance. Our holding today does not assume that patient action is attributable to a prescribing physician solely because they have a physician-patient relationship. We leave to another day what other scenarios also satisfy the "direction or control" requirement. The two-prong test that we set forth in *Akamai V* is applicable to the facts of this case and resolves the existence of underlying direct infringement.

B

Although we conclude that the two-prong *Akamai V* test is met here, this does not end our inquiry. ***HN5***[⬆] "The mere existence of direct infringement by physicians, while necessary to find liability for induced infringement, is not sufficient for inducement." *Takeda Pharms. U.S.A., Inc. v. West-Ward Pharm. Corp., 785 F.3d 625, 631 (Fed. Cir. 2015)*. To show inducement, Eli Lilly carries the burden of further proving "specific intent and action to induce infringement." *Takeda, 785 F.3d at 631*. Mere "knowledge of the acts alleged to constitute infringement" is not sufficient. *DSU Med., 471 F.3d at 1305*.

As noted before, the district court **[**19]** found that the administration of folic acid before pemetrexed administration was "not merely a suggestion or recommendation, but a critical step." *Eli Lilly III, 126 F.*

---

[5] As Eli Lilly points out, nor did we rely on legal obligations or technological prerequisites to reach our decision in *Akamai V.* The standard contract in that case was not significant for imposing potential civil liability but for "delineat[ing] the steps" that customers would have to perform "if [they] wish[ed] to use [defendant's] product." *Akamai V, 797 F.3d at 1024*. And we did not focus on whether a customer's failure to perform certain steps might have made it technologically impossible for other steps to occur. *Id.*

[6] Asserted claims 9, 12, 14, and 15 recite administering "about 350 µg to about 1000 µg" of folic acid. '209 patent col. 11 ll. 19-20, col. 11 l. 25-col. 12 l. 4, col. 12 ll. 7-11. Asserted claims 10, 18, and 19 recite administering "350 µg to 600 µg" of folic acid. *Id.* at col. 11 ll. 21-23, col. 12 ll. 16-20. Asserted claim 21 recites either of those folic acid dosage ranges. *Id.* at col. 12 ll. 24-27. Asserted claim 19 further recites a schedule for folic acid administration "wherein folic acid is administered 1 to 3 weeks prior to the first administration of the pemetrexed." *Id.* at col. 12 ll. 18-20.

Supp. 3d at 1042. It further held that Defendants induce physicians' infringement because physicians act "in accordance with Defendants' proposed labeling." *Id.* Accordingly, the district court concluded that Defendants would induce infringement of the '209 patent.

Defendants submit that, even if there is direct infringement, their product labeling does not induce such infringement. They argue that Eli Lilly has not offered any evidence of what physicians do "*in general*," offering instead only "speculation about how physicians *may* act." Appellants' Opening Br. 24 (second emphasis added). Furthermore, they submit that physicians "who merely follow the product label" are not induced to infringe because physicians must go beyond the labeling instructions—such as by prescribing specific doses of folic acid or requiring patients to keep "pill counts" or "pill diaries"—to infringe. *Id.* at 23, 26. We agree with Eli Lilly that Defendants' arguments are unavailing.

[*1285]** We make two observations at the outset. First, to be clear, **HN6**[↑] the intent for inducement must be with respect to the actions of **[**20]** the underlying direct infringer, here physicians. Second, we have not required evidence regarding the general prevalence of the induced activity. When the alleged inducement relies on a drug label's instructions, "[t]he question is not just whether [those] instructions describ[e] the infringing mode, . . . but whether the instructions teach an infringing use *such that* we are willing to infer from those instructions an affirmative intent to infringe the patent." Takeda, 785 F.3d at 631 (internal quotation marks omitted). "The label must encourage, recommend, or promote infringement." *Id.* For purposes of inducement, "it is irrelevant that some users may ignore the warnings in the proposed label." AstraZeneca LP v. Apotex, Inc., 633 F.3d 1042, 1060 (Fed. Cir. 2010).

Depending on the clarity of the instructions, the decision to continue seeking FDA approval of those instructions may be sufficient evidence of specific intent to induce infringement. Id. at 1059. With respect to those instructions, we held in *AstraZeneca* that a label that instructed users to follow the instructions in an infringing manner was sufficient even **[*1369]** though some users would not follow the instructions. Id. at 1059-60. This was true even though the product in question had substantial noninfringing uses. *Id.*

Conversely, "vague" instructions that **[**21]** require one to "look outside the label to understand the alleged implicit encouragement" do not, without more, induce infringement. Takeda, 785 F.3d at 632, 634. Defendants try to analogize the product labeling here to the labeling in *Takeda* that we held did not provide clear enough instructions for the infringing use to show inducement. *Takeda*, however, is distinguishable. The generic manufacturer in that case sought FDA approval for a generic drug to be used as a prophylaxis for gout flares—a use not covered by the patents that had been asserted. Id. at 628. The only link between the proposed use described on the labeling and the patented use was an instruction stating, "[i]f you have a gout flare while taking [the drug], tell your healthcare provider." Id. at 632 (first alteration in original) (internal quotation marks omitted). The patent owner argued that physicians who are accordingly consulted might prescribe the drug for the infringing, off-label use and that the accused infringer was willfully blind to this possibility. *Id.* We rejected the patent owner's reliance on such "vague label language" and "speculation about how physicians may act." *Id.* The product labeling here is not so tenuously related to the use covered by the **[**22]** asserted claims, and Eli Lilly does not need to rely on speculation about physician behavior.

Again, the product labeling includes repeated instructions and warnings regarding the importance of and reasons for folic acid treatment, and there is testimony that the Physician Prescribing Information, as the name indicates, is directed at physicians. *See* J.A. 2181, 11253, 11255, 11256, 11258, 11278. The instructions are unambiguous on their face and encourage or recommend infringement.

Defendants rely heavily on evidence that physicians as a matter of practice take steps beyond the instructions in the product labeling, such as asking patients to keep pill diaries or pill counts, or confirming compliance with folic acid administration. For example, they point to Dr. Chabner's testimony that he gives patients instructions "beyond what the instruction is in th[e] patient information." J.A. 2235-36. But the asserted claims do not recite additional steps such as pill diaries, pill counts, and compliance measures. **HN7**[↑] Where the product labeling already encourages infringement of the asserted claims, as it does here, a physician's decision to give patients even more specific guidance is irrelevant to the **[**23]** question of inducement.[7]

[7] As Dr. Chabner testified, such additional instructions are rightfully "left to the medical judgment of [the] doctor," depending on the circumstances. J.A. 2231.

In sum, evidence that the product labeling that Defendants seek would inevitably lead some physicians to infringe establishes the requisite intent for inducement. The district court did not clearly err in concluding that Defendants would induce infringement of the asserted claims of the '209 patent.

II

We turn next to the district court's holding that the limitation "vitamin B12" was not indefinite. ***HN8***[↑] Pursuant to *35 U.S.C. § 112*, ¶ 2, a patent specification must "conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention."[8] The district **[*1370]** court considered the indefiniteness of **[***1286]** the asserted claims before the Supreme Court changed the relevant standard in *Nautilus, Inc. v. Biosig Instruments, Inc., 134 S. Ct. 2120, 189 L. Ed. 2d 37 (2014)*, and held that "vitamin B12" was not indefinite.[9] *Eli Lilly & Co. v. Teva Parenteral Meds., Inc. (Eli Lilly I), No. 1:10-cv-1376-TWP-DKL, 2012 U.S. Dist. LEXIS 85369, 2012 WL 2358102, at *11-12 (S.D. Ind. June 20, 2012)*. The district court further construed "vitamin B12" to mean "cyanocobalamin," a particular vitamin supplement. *2012 U.S. Dist. LEXIS 85369, [WL] at *12*.

HN9[↑] In *Nautilus*, the Supreme Court rejected our "not amenable to construction or insolubly ambiguous" standard for indefiniteness and articulated, instead, that "a patent is invalid for indefiniteness if its claims, **[**24]** read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *134 S. Ct. at 2124*. Indefiniteness is a question of law that we review de novo. *Teva Pharms. USA, Inc. v. Sandoz, Inc., 789 F.3d 1335, 1341 (Fed. Cir. 2015)*. We have reiterated post-*Nautilus* that "general principles of claim construction apply" to the question of indefiniteness. *Biosig Instruments, Inc. v. Nautilus, Inc., 783 F.3d 1374, 1377 (Fed. Cir. 2015)* (internal quotation marks omitted). Accordingly, we review subsidiary factual determinations made by the district court based on extrinsic evidence for clear error. *Id.*; *see also Teva, 789 F.3d at 1341-42* (reviewing subsidiary factual findings in the indefiniteness context for clear error).

The parties do not dispute that, depending on the context, "vitamin B12" can be used in the art to refer either to cyanocobalamin specifically or, more broadly, to a class of compounds including pharmaceutical derivatives of cyanocobalamin. The parties do not dispute that the written description of the '209 patent uses the term both ways.[10] Defendants argue that, because "vitamin B12" is used in two different ways in the intrinsic record, "it is impossible to determine" which meaning applies to the claims "with any reasonable certainty," as required by *Nautilus*. **[**25]** Appellants' Opening Br. 31. Eli Lilly counters that the claims of the '209 patent "involve administering a vitamin B_{12} supplement to a patient," and in that context, "the one and only meaning" of vitamin B12 to a person of ordinary skill is cyanocobalamin. Appellee's Br. 35.

The district court expressly "accept[ed]" the testimony of Eli Lilly's expert, Dr. O'Dwyer, who concluded that a person of ordinary skill would understand "vitamin B12" to mean cyanocobalamin in the context of the patent claims. *Eli Lilly I, 2012 U.S. Dist. LEXIS 85369, 2012 WL 2358102, at *11*. We do not defer to Dr. O'Dwyer's "ultimate conclusion **[*1371]** about claim meaning in the context of th[e] patent," as that is a legal question. *Teva, 789 F.3d at 1342*. But the district court's underlying determination, based on extrinsic evidence, of what a person of ordinary skill would understand "vitamin B12" to mean in different contexts is a question of fact. *See id.* (***HN10***[↑] "Understandings that lie outside the patent documents about the meaning of terms to one of skill in the art or the science or state of the knowledge of one of skill in the art are factual issues."). Dr. O'Dwyer testified that, although "vitamin

---

[8] Paragraph 2 of *35 U.S.C. § 112* was replaced with *§ 112(b)* by *§ 4(c)* of the AIA, and § 4(e) makes that change applicable "to any patent application that is filed on or after" September 16, 2012. ***Pub. L. No. 112-29, § 4, 125 Stat. at 296-97***. Because the application resulting in the '209 patent was filed before that date, we refer to the pre-AIA version of *§ 112*.

[9] Under the prevailing standard at the time, a term was indefinite only if it was "not amenable to construction" or was "insolubly ambiguous." *Datamize, LLC v. Plumtree Software, Inc., 417 F.3d 1342, 1347 (Fed. Cir. 2005)* (internal quotation marks omitted), *overruled by Nautilus, 134 S. Ct. at 2124*.

[10] The specification provides that "[t]he term 'vitamin B12' refers to vitamin B12 and its pharmaceutical derivatives," and that "[p]referably the term refers to vitamin B12, cobalamin, and chlorocobalamin." '209 patent col. 5 ll. 5-10. The district court held, and Defendants do not dispute on appeal, that this language did not signify that the patentee was redefining the term "vitamin B12." *Eli Lilly I, 2012 U.S. Dist. LEXIS 85369, 2012 WL 2358102, at *10-11*.

B12" can refer to a class of compounds in other contexts, it refers specifically to cyanocobalamin when "vitamin B12" is prescribed **[**26]** in the medical field. *See, e.g.*, J.A. 3571 ("'Vitamin B12' is used by medical oncologists to mean a particular vitamin supplement, and medical oncologists refer to 'vitamin B12,' and prescribe 'vitamin B12,' without further explanation or definition."). We see no clear error in the district court's acceptance of the understanding that "vitamin B12," when used to refer to vitamin B12 supplementation in a medical context, refers to cyanocobalamin.[11] In view of this understanding, **[***1287]** and because the specification uses "vitamin B12" primarily in two ways, we do not face the problem that we did in *Teva*, in which the disputed term did "not have a plain meaning to one of skill in the art" that could be determined from context. *789 F.3d at 1345*.

The claim language here would inform a person of ordinary skill that the term "vitamin B12," as used in the '209 patent claims, refers to "cyanocobalamin." First, the claims, on their face, are directed to administering vitamin supplements, including vitamin B12, followed by chemotherapy treatment. This context informs persons of ordinary skill that "vitamin B12" is being used to refer to the supplementation form of vitamin B12, cyanocobalamin. Second, the structure of the claims **[**27]** also supports such an understanding. Claim 1 requires administering a "methylmalonic acid lowering agent . . . selected from the group consisting of," inter alia, vitamin B12 and cyanocobalamin. '209 patent col. 10 ll. 61-65. Claim 2, which depends from claim 1, further requires that "the methylmalonic acid lowering agent is vitamin B12." *Id.* at col. 10 ll. 66-67. Eli Lilly asserts, and Defendants do not dispute, that if "vitamin B12" were to refer to a class of compounds, then claim 2 would be the same scope as claim 1, as claim 2 "would encompass the same methylmalonic acid lowering agents set forth in claim 1." Appellee's Br. 36. ***HN11***[↑] The doctrine of claim differentiation, however, presumes that dependent claims are "of narrower scope than the independent claims from which they depend." *AK Steel Corp. v. Sollac & Ugine, 344 F.3d 1234, 1242 (Fed. Cir. 2003)*. Reading the claims to require "vitamin B12" to be a specific compound in the class of "methylmalonic acid lowering agents" would avoid this problem, as it would render claim 2, and all of the claims that depend from it, narrower than claim 1.

Defendants submit that, if "vitamin B12" means "cyanocobalamin," then claim 1 recites a Markush group of "methylmalonic acid lowering agents" that lists the same compound **[**28]** twice. ***HN12***[↑] Although we have in some instances interpreted claim terms to avoid redundancy, "the rule is not inflexible." *Power Mosfet Techs., LLC v. Siemens AG, 378 F.3d 1396, 1409-10 (Fed. **[*1372]** Cir. 2004)*; *see also Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp., 831 F.3d 1350, 1363-64 (Fed. Cir. 2016)*; Manual of Patent Examining Procedure § 2173.05(h)(I) ("The mere fact that a compound may be embraced by more than one member of a Markush group recited in the claim does not necessarily render the scope of the claim unclear."). Here, the redundancy is supported by the prosecution history, during which the examiner stated that vitamin B12 and cyanocobalamin "are the same" agents. J.A. 4239. Therefore, faced with an interpretation that would read redundancy into claim 1 and another that would violate the doctrine of claim differentiation, we hold that the claims here support the former result over the latter.

We are not persuaded by Defendants' contention that the prosecution history fails to "provide reasonable confidence in any particular meaning of the term 'vitamin B12.'" Appellants' Opening Br. 30. In response to the examiner's statement that "vitamin B12" and "cyanocobalamin" are synonymous, the patentee initially removed the term "cyanocobalamin" from the proposed claims. *See* J.A. 4825-27, 4832-33. Later during prosecution, the patentee added "cyanocobalamin" back **[**29]** into the claim that eventually issued as claim 1. J.A. 4836. Defendants do not point to any reason, though, that a person of ordinary skill would understand the patentee's decision to ultimately include "cyanocobalamin" in the claim language to be a departure from the understanding expressed by the examiner that "vitamin B12" and "cyanocobalamin" refer to the same compound. The prosecution history here does not detract from, and is consistent with, the other intrinsic evidence that would inform a skilled artisan regarding the scope of the claim term "vitamin B12."

We therefore hold that a person of ordinary skill in the art would understand the scope of the claim term "vitamin B12" with reasonable certainty. Applying *Nautilus* in this case does not lead us to a different result from the district court's conclusion on the question of indefiniteness.

III

[11] Indeed, Defendants' expert, Dr. Green, agreed that "in the strict biochemical nomenclature, the term 'vitamin B12' is restricted to cyanocobalamin," J.A. 3767, and that it can refer specifically to cyanocobalamin in the context of vitamin B12 injections, J.A. 3748-49.

Next, we address Defendants' arguments that the asserted claims were obvious over several references that are not disputed to be prior art as of the critical date in June 1999. ***HN13***[↑] To prevail on obviousness, an alleged infringer must prove by clear and convincing evidence "that a skilled artisan would have been motivated to combine the teachings **[**30]** of the prior art references to achieve the claimed invention, and that the skilled artisan would have had a reasonable expectation of success in doing so." *Procter & Gamble Co. v. Teva Pharm. USA, Inc., 566 F.3d 989, 994 [***1288] (Fed. Cir. 2009)* (internal quotation marks omitted). Obviousness is a question of law based on underlying facts, and "[o]n appeal from a bench trial, this court reviews the district court's conclusions of law de novo and findings of fact for clear error." *Prometheus Labs., Inc. v. Roxane Labs., Inc., 805 F.3d 1092, 1097 (Fed. Cir. 2015)* (internal quotation marks omitted).

In a thorough opinion, the district court found, inter alia, that a skilled artisan would not have been motivated to: (1) use folic acid pretreatment with pemetrexed; (2) use vitamin B12 pretreatment with pemetrexed; or (3) use the claimed doses and schedules of folic acid and vitamin B12 pretreatments with pemetrexed. The court also found that Eli Lilly had established several secondary considerations in favor of nonobviousness. On appeal, Defendants contend that all of those findings were erroneous. Eli Lilly submits that Defendants' **[*1373]** arguments "amount to nothing more than an effort to reargue the facts." Appellee's Br. 46.

We agree with Eli Lilly that Defendants' arguments fail to raise reversible error with respect to at least the findings that a skilled artisan **[**31]** would not have been motivated to use vitamin B12 pretreatment with pemetrexed, let alone the appropriate doses and schedules of such vitamin B12 pretreatment.

A

The district court found, based upon two abstracts published in 1998 by Dr. Niyikiza ("the Niyikiza abstracts"),[12] that a skilled artisan "would have concluded that vitamin B_{12} deficiency was not the problem in pemetrexed toxicity." *Eli Lilly & Co. v. Teva Parenteral Meds., Inc. (Eli Lilly II), No. 1:10-cv-01376-TWP-DWL, 2014 U.S. Dist. LEXIS 43885, 2014 WL 1350129, at *10 (S.D. Ind. Mar. 31, 2014)*. It further found that a skilled artisan would not have used vitamin B12 supplementation to address antifolate toxicities because of "concern[] about . . . a reduction of efficacy of the antifolate" treatment. *2014 U.S. Dist. LEXIS 43885, [WL] at *11*.

Dr. Niyikiza was an Eli Lilly scientist at the time and is the named inventor on the '209 patent. In 1997, he performed statistical analyses to try to determine which clinical trial patients were likely to develop toxicities from pemetrexed treatment. J.A. 1045, 1071-72. He published **[**32]** the results in the Niyikiza abstracts and reported a correlation between increased pemetrexed toxicities and elevated homocysteine levels. J.A. 7948, 7950-51. Elevated homocysteine levels serve as an indicator of either a folic acid or vitamin B12 deficiency, but they do not indicate which of those two vitamins is specifically lacking. J.A. 622, 719, 7910. Levels of another marker, methylmalonic acid ("MMA"), serve more specifically as an indicator of vitamin B12 deficiency. J.A. 720. But the Niyikiza abstracts reported that "no correlation between toxicity . . . and [MMA levels] was seen." J.A. 7948.

Given the toxicity correlations that Dr. Niyikiza observed with homocysteine levels but not with MMA levels, Eli Lilly's experts testified that the Niyikiza abstracts "present[ed] no evidence for a relationship of vitamin B12 and pemetrexed toxicity" and would not have motivated a skilled artisan to administer vitamin B12 to patients to address pemetrexed toxicity. J.A. 1466-67; *see also* J.A. 1475, 1942. Defendants' expert, Dr. Ratain, confirmed that if a patient exhibits elevated homocysteine but normal MMA levels, a skilled artisan "would conclude that that patient was folate deficient" but "not **[**33]** [vitamin] B12 deficient." J.A. 622-23.

To try to overcome this missing link between vitamin B12 deficiency and pemetrexed toxicity, Defendants turn to other prior art references. They argue that, based on those references and perhaps preexisting knowledge, a person of ordinary skill would have known that folate deficiency is correlated with pemetrexed toxicity and that vitamin B12 "directly affect[s] the amount of folate available to healthy cells." Appellants' Opening Br. 45 (citing J.A. 2482, 7894, 7910-11, 8086). As a result, they argue, skilled artisans would have been motivated to use vitamin B12, along with folic acid, to address pemetrexed toxicities. *Id.* Put another way, if

---

[12] C. Niyikiza et al., *LY231514 (MTA): Relationship of Vitamin Metabolite Profile to Toxicity*, 17 PROC. OF AM. SOCIETY OF CLINICAL ONCOLOGY 558a, Abstract 2139 (1998); C. Niyikiza et al., *MTA (LY231514): Relationship of Vitamin Metabolite Profile, Drug Exposure, and Other Patient Characteristics to Toxicity*, 9 ANNALS OF ONCOLOGY 126, Abstract 609P (4th Supp. 1998).

[*1374] we assume that the prior art would have motivated skilled artisans to use folic acid pretreatment to counter pemetrexed toxicity (an issue we do not reach), Defendants submit that those skilled artisans would have also used vitamin B12 as part of the pretreatment because the biochemical pathways for vitamin B12 and folic acid are related. Defendants further submit that other prior art "expressly teaches that folic acid supplementation *improves* the therapeutic index **[***1289]** of pemetrexed," so a skilled artisan would not have **[**34]** been concerned about using vitamin B12 supplementation to reduce pemetrexed toxicities. *Id.* at 46.

But the parties' experts agreed that nothing in the literature as of the critical date described "cancer patients being provided with vitamin B12 supplementation prior to receiving any antifolate," with or without folic acid. J.A. 597-98; *see also* J.A. 1957. Defendants fail to point to evidence that, even if folic acid supplementation were known to improve effects of pemetrexed treatment, a skilled artisan would have thought the same of vitamin B12. Indeed, Eli Lilly offered expert testimony that a skilled artisan would have viewed the use of vitamin B12 with antifolates as "a problem" based on "having to increase the [antifolate] dose to get the same activity" of cancer treatment. J.A. 1453-54.

We are therefore not convinced that the district court committed clear error in concluding that Defendants failed to carry their burden of proving that it would have been obvious to a person of ordinary skill to use vitamin B12 pretreatment to reduce pemetrexed toxicities.

B

Regarding the dose and schedule of vitamin B12, the district court reiterated that "there are no prior art references where *any amount* ***[**35]*** of vitamin B_{12} pretreatment had been used with an antifolate in the treatment of cancer." *Eli Lilly II, 2014 U.S. Dist. LEXIS 43885, 2014 WL 1350129, at *13* (emphasis added). The court also discounted Defendants' citations to literature outside the field of oncology. *2014 U.S. Dist. LEXIS 43885, [WL] at *13-14*.

Defendants argue that, "[o]nce a [skilled artisan] is motivated to use vitamin B12 pretreatment," selecting a dose and schedule for vitamin B12 "would have been routine." Appellants' Opening Br. 47. Setting aside motivation to use vitamin B12 pretreatment in the first instance, Defendants only cite evidence of vitamin B12 doses and schedules that are "routine" in other medical contexts. *See, e.g.*, J.A. 8150, 8169, 756-57. There is no evidence that, considering the context of pemetrexed treatment and associated toxicity problems, a person of ordinary skill would have applied such doses and schedules wholesale.

We therefore also see no clear error in the court's finding that Defendants failed to carry their burden of proving that the prior art disclosed the claimed doses and schedules of vitamin B12 for purposes of pemetrexed pretreatment.

C

Defendants make two additional, overarching arguments that we also find unavailing.

First, Defendants cite *PharmaStem Therapeutics, Inc. v. ViaCell, Inc., 491 F.3d 1342 (Fed. Cir. 2007)*, to argue that the district court erred by accepting **[**36]** expert testimony that was inconsistent with the express disclosures of the prior art. But *PharmaStem* is distinguishable. In that case, we discounted testimony regarding prior art references that "[could not] be reconciled with statements made by the inventors in the joint specification [of the asserted patents] and with the prior art references themselves." *Id. at 1361*. Here, despite Defendants' averments, we do not perceive any irreconcilable differences between **[*1375]** the prior art disclosures on their face and the testimony regarding whether a person of ordinary skill would have been motivated to use vitamin B12 pretreatment in the claimed doses and schedules with pemetrexed treatment.

Second, Defendants argue that the district court committed legal error by requiring an express prior art disclosure of the claimed combination because *KSR International Co. v. Teleflex Inc., 550 U.S. 398, 127 S. Ct. 1727, 167 L. Ed. 2d 705 (2007)*, rejected such a "rigid" formula in favor of a more flexible inquiry. *Id. at 402-03*. While *KSR* did make the obviousness inquiry more flexible, it does not advance Defendants' position here. Defendants cite to two prior art references that would purportedly "motivate a [skilled artisan] to review literature regarding known doses and schedules for vitamin B12 supplementation." Appellants' **[**37]** Opening Br. 51. But those references merely note in passing that vitamin B12 can be related to homocysteine levels and folate biochemical pathways. *See* J.A. 7894, 7910. Defendants do not cite to any testimony to support their contention that those references would motivate a skilled artisan to arrive at the claimed use of vitamin B12 as a pretreatment for

pemetrexed, especially in view of the evidence of gaps and concerns regarding the prior art discussed above.

The district court did not commit reversible error in finding that the prior art fails to render obvious use of vitamin B12 pretreatment with pemetrexed, or use of the doses and schedules of vitamin B12 that are recited in the asserted claims. We therefore affirm the **[***1290]** determination of nonobviousness. We need not reach the other grounds put forth for obviousness.

IV

Finally, we address Defendants' argument that the district court erred in holding that the asserted claims are not invalid for obviousness-type double patenting over U.S. Patent No. 5,217,974 ("'974 patent"), an earlier patent also owned by Eli Lilly.

HN14[↑] The judicially-created "doctrine of obviousness-type double patenting is intended to 'prevent the extension of the term of a patent . . . by prohibiting the issuance **[**38]** of the claims in a second patent not patentably distinct from the claims of the first patent.'" *Eli Lilly & Co. v. Teva Parenteral Meds., Inc., 689 F.3d 1368, 1376 (Fed. Cir. 2012)* (alteration in original) (quoting *In re Longi, 759 F.2d 887, 892 (Fed. Cir. 1985))*. After determining the differences in the claims of the earlier and later patents, the court must determine if the alleged infringer has proven by clear and convincing evidence that the claims are not patentably distinct. *Eli Lilly & Co. v. Barr Labs., Inc., 251 F.3d 955, 962, 968 (Fed. Cir. 2001)*. "A later patent claim is not patentably distinct from an earlier claim if the later claim is obvious over, or anticipated by, the earlier claim." *Id.* Even where a patent is found invalid for obviousness-type double patenting, though, a patentee may file a terminal disclaimer. *Boehringer Ingelheim Int'l GmbH v. Barr Labs., Inc., 592 F.3d 1340, 1347 (Fed. Cir. 2010)*; *see also Perricone v. Medicis Pharm. Corp., 432 F.3d 1368, 1375 (Fed. Cir. 2005)* (noting that there is no "prohibition on post-issuance terminal disclaimers" and that "[a] terminal disclaimer can indeed supplant a finding of invalidity for double patenting"). Obviousness-type double patenting is a question of law based on underlying facts, so "[o]n appeal from a bench trial, this court reviews the district court's conclusions of law de novo and findings of fact for clear error." *Prometheus, 805 F.3d at 1097* (internal quotation marks omitted).

Defendants argued to the district court that the asserted claims of the '209 patent **[*1376]** are obvious variants of claim 20 of the '974 patent. The court **[**39]** found that the asserted claims differ from claim 20 of the '974 patent "in that the Asserted Claims limit the drug to pemetrexed and the administration to a patient, use a dose range for folic acid of 350-1000 µg or 350-600 µg and add[] vitamin B12, whereas claim 20 of the '974 Patent discloses the use of a much greater amount of folic acid—500-30,000 µg—with an antifolate . . . administered to a mammal." *Eli Lilly II, 2014 U.S. Dist. LEXIS 43885, 2014 WL 1350129, at *17*. In particular, the '974 patent lacks any recitation of vitamin B12 pretreatment, let alone dosage ranges or schedules of such pretreatment.

For many of the same reasons it articulated in its obviousness analysis and with additional explanation, the district court found that the use of pemetrexed, use of vitamin B_{12}, and doses and schedules of the asserted claims were patentably distinct from claim 20 of the '974 patent. *2014 U.S. Dist. LEXIS 43885, [WL] at *17-18*. In relevant part, the district court held that, "as previously discussed, there would have been no reason for a [skilled artisan] to add vitamin B12 to the folic acid pretreatment." *2014 U.S. Dist. LEXIS 43885, [WL] at *17*. For the same reasons that we discussed with respect to nonobviousness, the court did not err in finding that those limitations regarding vitamin B12 would not have been obvious to a person of ordinary skill.

Therefore, we affirm **[**40]** the district court's conclusion that the asserted claims are not invalid for obviousness-type double patenting.

CONCLUSION

For the foregoing reasons, we affirm the district court's judgment.

AFFIRMED

End of Document

Notices

Federal Register
Vol. 84, No. 4
Monday, January 7, 2019

This section of the FEDERAL REGISTER contains documents other than rules or proposed rules that are applicable to the public. Notices of hearings and investigations, committee meetings, agency decisions and rulings, delegations of authority, filing of petitions and applications and agency statements of organization and functions are examples of documents appearing in this section.

DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

[Docket No. PTO–P–2018–0053]

2019 Revised Patent Subject Matter Eligibility Guidance

AGENCY: United States Patent and Trademark Office, Commerce.

ACTION: Examination Guidance; Request for comments.

SUMMARY: The United States Patent and Trademark Office (USPTO) has prepared revised guidance (2019 Revised Patent Subject Matter Eligibility Guidance) for use by USPTO personnel in evaluating subject matter eligibility. The 2019 Revised Patent Subject Matter Eligibility Guidance revises the procedures for determining whether a patent claim or patent application claim is directed to a judicial exception (laws of nature, natural phenomena, and abstract ideas) under Step 2A of the USPTO's Subject Matter Eligibility Guidance in two ways. First, the 2019 Revised Patent Subject Matter Eligibility Guidance explains that abstract ideas can be grouped as, *e.g.,* mathematical concepts, certain methods of organizing human activity, and mental processes. Second, this guidance explains that a patent claim or patent application claim that recites a judicial exception is not ''directed to'' the judicial exception if the judicial exception is integrated into a practical application of the judicial exception. A claim that recites a judicial exception, but is not integrated into a practical application, is directed to the judicial exception under Step 2A and must then be evaluated under Step 2B (inventive concept) to determine the subject matter eligibility of the claim. The USPTO is seeking public comment on its subject matter eligibility guidance, and particularly the 2019 Revised Patent Subject Matter Eligibility Guidance.

DATES: *Applicable Date:* The 2019 Revised Patent Subject Matter Eligibility Guidance is effective on January 7, 2019. The 2019 Revised Patent Subject Matter Eligibility Guidance applies to all applications, and to all patents resulting from applications, filed before, on, or after January 7, 2019.

Comment Deadline Date: Written comments must be received on or before March 8, 2019.

ADDRESSES: Comments must be sent by electronic mail message over the internet addressed to: *Eligibility2019@uspto.gov.*

Electronic comments submitted in plain text are preferred, but also may be submitted in ADOBE® portable document format or MICROSOFT WORD® format. Comments not submitted electronically should be submitted on paper in a format that facilitates convenient digital scanning into ADOBE® portable document format. The comments will be available for viewing via the USPTO's internet website (*http://www.uspto.gov*). Because comments will be made available for public inspection, information that the submitter does not desire to make public, such as an address or phone number, should not be included in the comments.

FOR FURTHER INFORMATION CONTACT: June E. Cohan, Senior Legal Advisor, at 571–272–7744 or Carolyn Kosowski, Senior Legal Advisor, at 571–272–7688, both with the Office of Patent Legal Administration.

SUPPLEMENTARY INFORMATION: Patent subject matter eligibility under 35 U.S.C. 101 has been the subject of much attention over the past decade. Recently, much of that attention has focused on how to apply the U.S. Supreme Court's framework for evaluating eligibility (often called the *Alice/Mayo* test).[1] Properly applying the *Alice/Mayo* test in a consistent manner has proven to be difficult, and has caused uncertainty in this area of the law. Among other things, it has become difficult in some cases for inventors, businesses, and other patent stakeholders to reliably and predictably determine what subject matter is patent-eligible. The legal uncertainty surrounding Section 101 poses unique challenges for the USPTO, which must ensure that its more than 8500 patent examiners and administrative patent judges apply the *Alice/Mayo* test in a manner that produces reasonably consistent and predictable results across applications, art units and technology fields.

Since the *Alice/Mayo* test was announced and began to be extensively applied, the courts and the USPTO have tried to consistently distinguish between patent-eligible subject matter and subject matter falling within a judicial exception. Even so, patent stakeholders have expressed a need for more clarity and predictability in its application. In particular, stakeholders have expressed concern with the proper scope and application of the ''abstract idea'' exception. Some courts share these concerns, for example as demonstrated by several recent concurrences and dissents in the U.S. Court of Appeals for the Federal Circuit (''Federal Circuit'') calling for changes in the application of Section 101 jurisprudence.[2] Many stakeholders, judges, inventors, and practitioners across the spectrum have argued that something needs to be done to increase clarity and consistency in how Section 101 is currently applied.

To address these and other concerns, the USPTO is revising its examination procedure with respect to the first step of the *Alice/Mayo* test [3] (Step 2A of the USPTO's Subject Matter Eligibility Guidance as incorporated into the Manual of Patent Examining Procedure (''MPEP'') 2106) [4] by: (1) Providing groupings of subject matter that is considered an abstract idea; and (2) clarifying that a claim is not ''directed to'' a judicial exception if the judicial exception is integrated into a practical application of that exception.

[1] *Alice Corp. Pty. Ltd.* v. *CLS Bank Int'l,* 573 U.S. 208, 217–18 (2014) (citing *Mayo Collaborative Servs.* v. *Prometheus Labs., Inc.,* 566 U.S. 66 (2012)).

[2] *See, e.g., Interval Licensing LLC,* v. *AOL, Inc.,* 896 F.3d 1335, 1348 (Fed. Cir. 2018) (Plager, J., concurring in part and dissenting in part); *Smart Sys. Innovations, LLC* v. *Chicago Transit Auth.,* 873 F.3d 1364, 1377 (Fed. Cir. 2017) (Linn, J., dissenting in part and concurring in part); *Berkheimer* v. *HP Inc.,* 890 F.3d 1369, 1376 (Fed. Cir. 2018) (Lourie, J., joined by Newman, J., concurring in denial of rehearing en banc).

[3] The first step of the *Alice/Mayo* test is to determine whether the claims are ''directed to'' a judicial exception. *Alice,* 573 U.S. at 217 (citing *Mayo,* 566 U.S. at 77).

[4] All references to the MPEP in the 2019 Revised Patent Subject Matter Eligibility Guidance are to the Ninth Edition, Revision 08–2017 (rev. Jan. 2018), unless otherwise indicated.

Section I of this 2019 Revised Patent Subject Matter Eligibility Guidance explains that the judicial exceptions are for subject matter that has been identified as the ''basic tools of scientific and technological work,'' [5] which includes ''abstract ideas'' such as mathematical concepts, certain methods of organizing human activity, and mental processes; as well as laws of nature and natural phenomena. Only when a claim recites a judicial exception does the claim require further analysis in order to determine its eligibility. The groupings of abstract ideas contained in this guidance enable USPTO personnel to more readily determine whether a claim recites subject matter that is an abstract idea.

Section II explains that the USPTO has set forth a revised procedure, rooted in Supreme Court caselaw, to determine whether a claim is ''directed to'' a judicial exception under the first step of the *Alice/Mayo* test (USPTO Step 2A).

Section III explains the revised procedure that will be applied by the USPTO. The procedure focuses on two aspects of Revised Step 2A: (1) Whether the claim recites a judicial exception; and (2) whether a recited judicial exception is integrated into a practical application. Only when a claim recites a judicial exception and fails to integrate the exception into a practical application, is the claim ''directed to'' a judicial exception, thereby triggering the need for further analysis pursuant to the second step of the *Alice/Mayo* test (USPTO Step 2B). Finally, if further analysis at Step 2B is needed (for example to determine whether the claim merely recites well-understood, routine, conventional activity), this 2019 Revised Patent Subject Matter Eligibility Guidance explains that the examiner or administrative patent judge will proceed in accordance with existing USPTO guidance as modified in April 2018.[6]

The USPTO is seeking public comment on its subject matter eligibility guidance, and particularly the 2019 Revised Patent Subject Matter Eligibility Guidance. The USPTO is determined to continue its mission to provide predictable and reliable patent rights in accordance with this rapidly evolving area of the law. The USPTO's ultimate goal is to draw distinctions between claims to principles in the abstract and claims that integrate those principles into a practical application. To that end, the USPTO may issue further guidance, or modify the current guidance, in the future based on its review of the comments received, further experience of the USPTO and its stakeholders, and additional judicial actions. Implementation of examination guidance on eligibility is an iterative process and may continue with periodic supplements. The USPTO invites the public to submit suggestions on eligibility-related topics to address in future guidance supplements as part of their comments on the USPTO's subject matter eligibility guidance.

Impact on Examination Procedure and Prior Examination Guidance: This 2019 Revised Patent Subject Matter Eligibility Guidance supersedes MPEP 2106.04(II) (Eligibility Step 2A: Whether a Claim Is Directed to a Judicial Exception) to the extent it equates claims ''reciting'' a judicial exception with claims ''directed to'' a judicial exception, along with any other portion of the MPEP that conflicts with this guidance. A chart identifying portions of the MPEP that are affected by this guidance will be available for viewing via the USPTO's internet website (*http://www.uspto.gov*). This 2019 Revised Patent Subject Matter Eligibility Guidance also supersedes all versions of the USPTO's ''Eligibility Quick Reference Sheet Identifying Abstract Ideas'' (first issued in July 2015 and updated most recently in July 2018). Eligibility-related guidance issued prior to the Ninth Edition, R–08.2017, of the MPEP (published Jan. 2018) should not be relied upon. However, any claim considered patent eligible under prior guidance should be considered patent eligible under this guidance.

This guidance does not constitute substantive rulemaking and does not have the force and effect of law. The guidance sets out agency policy with respect to the USPTO's interpretation of the subject matter eligibility requirements of 35 U.S.C. 101 in view of decisions by the Supreme Court and the Federal Circuit. The guidance was developed as a tool for internal USPTO management and does not create any right or benefit, substantive or procedural, enforceable by any party against the USPTO. Rejections will continue to be based upon the substantive law, and it is those rejections that are appealable to the Patent Trial and Appeal Board (PTAB) and the courts. All USPTO personnel are, as a matter of internal agency management, expected to follow the guidance. Failure of USPTO personnel to follow the guidance, however, is not, in itself, a proper basis for either an appeal or a petition.

I. Groupings of Abstract Ideas

The Supreme Court has held that the patent eligibility statute, Section 101, contains an implicit exception for ''[l]aws of nature, natural phenomena, and abstract ideas,'' which are ''the basic tools of scientific and technological work.'' [7] Yet, the Court has explained that ''[a]t some level, all inventions embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas,'' and has cautioned ''to tread carefully in construing this exclusionary principle lest it swallow all of patent law.'' [8]

Since the *Alice* case, courts have been ''compare[ing] claims at issue to those claims already found to be directed to an abstract idea in previous cases.'' [9] Likewise, the USPTO has issued guidance to the patent examining corps about Federal Circuit decisions applying the *Alice/Mayo* test, for instance describing the subject matter claimed in the patent in suit and noting whether or not certain subject matter has been identified as an abstract idea.[10]

[5] *Mayo,* 566 U.S. at 71 (''Phenomena of nature, though just discovered, mental processes, and abstract intellectual concepts are not patentable, as they are the basic tools of scientific and technological work'' (quoting *Gottschalk* v. *Benson,* 409 U.S. 63, 67 (1972)).

[6] USPTO Memorandum of April 19, 2018, ''Changes in Examination Procedure Pertaining to Subject Matter Eligibility, Recent Subject Matter Eligibility Decision (*Berkheimer* v. *HP, Inc.*)'' (Apr. 19, 2018), *available at https://www.uspto.gov/sites/default/files/documents/memo-berkheimer-20180419.PDF* [hereinafter ''USPTO *Berkheimer* Memorandum''].

[7] *Alice Corp.,* 573 U.S. at 216 (internal citation and quotation marks omitted); *Mayo,* 566 U.S. at 71.

[8] *Id.* (internal citation and quotation marks omitted).

[9] *See Enfish, LLC* v. *Microsoft Corp.,* 822 F.3d 1327, 1334 (Fed. Cir. 2016); *see also Amdocs (Israel) Ltd.* v. *Openet Telecom, Inc.,* 841 F.3d 1288, 1294 (Fed. Cir. 2016) (''[T]he decisional mechanism courts now apply [to identify an abstract idea] is to examine earlier cases in which a similar or parallel descriptive nature can be seen—what prior cases were about, and which way they were decided.'').

[10] *See, e.g.,* 2014 Interim Guidance on Subject Matter Eligibility, 79 FR 74618, 74628–32 (Dec. 16, 2014) (discussing concepts identified as abstract ideas); July 2015 Update: Subject Matter Eligibility (Jul. 30, 2015), at 3–5, *available at https://www.uspto.gov/sites/default/files/documents/ieg-july-2015-update.pdf* (same); USPTO Memorandum of May 19, 2016, ''Recent Subject Matter Eligibility Decisions (*Enfish, LLC* v. *Microsoft Corp.* and *TLI Communications LLC* v. *A.V. Automotive, LLC*),'' at 2 (May 19, 2016), *available at https://www.uspto.gov/sites/default/files/documents/ieg-may-2016_enfish_memo.pdf* [hereinafter, ''USPTO *Enfish* Memorandum''] (discussing the abstract idea in *TLI Communications LLC* v. *A.V. Automotive, LLC,* 823 F.3d 607 (Fed. Cir. 2016)); USPTO Memorandum of November 2, 2016, ''Recent Subject Matter Eligibility Decisions,'' at 2 (Nov. 2, 2016), *available at https://www.uspto.gov/sites/default/files/documents/McRo-Bascom-Memo.pdf* [hereinafter, ''USPTO *McRo* Memorandum''] (discussing how the claims in *McRO, Inc.* v. *Bandai Namco Games America Inc.,* 837 F.3d 1299 (Fed. Cir. 2016), were directed to an improvement instead of an abstract idea); USPTO Memorandum of April 2, 2018, ''Recent Subject Matter Eligibility Decisions'' (Apr. 2, 2018), *available at https://www.uspto.gov/sites/default/files/documents/memo-recent-sme-ctdec-20180402.PDF* [hereinafter

Continued

While that approach was effective soon after *Alice* was decided, it has since become impractical. The Federal Circuit has now issued numerous decisions identifying subject matter as abstract or non-abstract in the context of specific cases, and that number is continuously growing. In addition, similar subject matter has been described both as abstract and not abstract in different cases.[11] The growing body of precedent has become increasingly more difficult for examiners to apply in a predictable manner, and concerns have been raised that different examiners within and between technology centers may reach inconsistent results.

The USPTO, therefore, aims to clarify the analysis. In accordance with judicial precedent and in an effort to improve consistency and predictability, the 2019 Revised Patent Subject Matter Eligibility Guidance extracts and synthesizes key concepts identified by the courts as abstract ideas to explain that the abstract idea exception includes the following groupings of subject matter, when recited as such in a claim limitation(s) (that is, when recited on their own or per se):

(a) Mathematical concepts—mathematical relationships, mathematical formulas or equations, mathematical calculations; [12]

(b) Certain methods of organizing human activity—fundamental economic principles or practices (including hedging, insurance, mitigating risk); commercial or legal interactions (including agreements in the form of contracts; legal obligations; advertising, marketing or sales activities or behaviors; business relations); managing personal behavior or relationships or interactions between people (including social activities, teaching, and following rules or instructions); [13] and

(c) Mental processes—concepts performed in the human mind [14] (including an observation, evaluation, judgment, opinion).[15]

''USPTO *Finjan* Memorandum''] (discussing how the claims in *Finjan Inc.* v. *Blue Coat Systems, Inc.,* 879 F.3d 1299 (Fed. Cir. 2018), and *Core Wireless Licensing, S.A.R.L.* v. *LG Electronics, Inc.,* 880 F.3d 1356 (Fed. Cir. 2018), were directed to improvements instead of abstract ideas); USPTO *Berkheimer* Memorandum at 2 (discussing the abstract idea in *Berkheimer*); MPEP 2106.04(a) (reviewing cases that did and did not identify abstract ideas).

[11] *E.g.,* compare *TLI Commc'ns,* 823 F.3d at 611, with *Enfish,* 822 F.3d at 1335, and *Visual Memory LLC* v. *NVIDIA Corp.,* 867 F.3d 1253, 1258 (Fed. Cir. 2017). While computer operations such as ''output of data analysis . . . can be abstract,'' *Credit Acceptance Corp.* v. *Westlake Servs.,* 859 F.3d 1044, 1056 (Fed. Cir. 2017), ''software-based innovations can [also] make 'non-abstract improvements to computer technology' and be deemed patent-eligible subject matter at step 1 [of the *Mayo/Alice* test],'' *Finjan,* 879 F.3d at 1304 (*quoting Enfish,* 822 F.3d at 1335). Indeed, the Federal Circuit has held that ''improvements in computer-related technology'' and ''claims directed to software'' are not ''inherently abstract.'' *Enfish,* 822 F.3d at 1335; *see also Visual Memory,* 867 F.3d at 1258. These developments in the caselaw can create complications for the patent-examination process. For example, claims in one application could be deemed to be abstract, whereas slightly different claims directed to the same or similar subject matter could be determined to reflect a patent eligible ''improvement.'' Alternatively, claims in one application could be found to be abstract, whereas claims to the same or similar subject matter in another application, containing additional or different embodiments in the specification, could be deemed eligible as not directed to an abstract idea. In other words, the finding that the subject matter claimed in a prior patent was ''abstract'' as claimed may not determine whether similar subject matter in another application, claimed somewhat differently or supported by a different disclosure, is directed to an abstract idea and therefore patent ineligible.

[12] *Bilski* v. *Kappos,* 561 U.S. 593, 611 (2010) (''The concept of hedging . . . reduced to a mathematical formula . . . is an unpatentable abstract idea[.]''); *Diamond* v. *Diehr,* 450 U.S. 175, 191 (1981) (''A mathematical formula as such is not accorded the protection of our patent laws'') (citing *Benson,* 409 U.S. 63); *Parker* v. *Flook,* 437 U.S. 584, 594 (1978) (''[T]he discovery of [a mathematical formula] cannot support a patent unless there is some other inventive concept in its application.''); *Benson,* 409 U.S. at 71–72 (concluding that permitting a patent on the claimed invention ''would wholly pre-empt the mathematical formula and in practical effect would be a patent on the algorithm itself''); *Mackay Radio & Telegraph Co.* v. *Radio Corp. of Am.,* 306 U.S. 86, 94 (1939) (''[A] scientific truth, or the mathematical expression of it, is not patentable invention[.]''); *SAP America, Inc.* v. *InvestPic, LLC,* 898 F.3d 1161, 1163 (Fed. Cir. 2018) (holding that claims to a ''series of mathematical calculations based on selected information'' are directed to abstract ideas); *Digitech Image Techs., LLC* v. *Elecs. for Imaging, Inc.,* 758 F.3d 1344, 1350 (Fed. Cir. 2014) (holding that claims to a ''process of organizing information through mathematical correlations'' are directed to an abstract idea); *Bancorp Servs., LLC* v. *Sun Life Assurance Co. of Can. (U.S.),* 687 F.3d 1266, 1280 (Fed. Cir. 2012) (identifying the concept of ''managing a stable value protected life insurance policy by performing calculations and manipulating the results'' as an abstract idea).

[13] *Alice,* 573 U.S. at 219–20 (concluding that use of a third party to mediate settlement risk is a ''fundamental economic practice'' and thus an abstract idea); *id.* (describing the concept of risk hedging identified as an abstract idea in *Bilski* as ''a method of organizing human activity''); *Bilski,* 561 U.S. at 611–612 (concluding that hedging is a ''fundamental economic practice'' and therefore an abstract idea); *Bancorp,* 687 F.3d at 1280 (concluding that ''managing a stable value protected life insurance policy by performing calculations and manipulating the results'' is an abstract idea); *Inventor Holdings, LLC* v. *Bed Bath & Beyond, Inc.,* 876 F.3d 1372, 1378–79 (Fed. Cir. 2017) (holding that concept of ''local processing of payments for remotely purchased goods'' is a ''fundamental economic practice, which *Alice* made clear is, without more, outside the patent system.''); *OIP Techs., Inc.* v. *Amazon.com, Inc.,* 788 F.3d 1359, 1362–63 (Fed. Cir. 2015) (concluding that claimed concept of ''offer-based price optimization'' is an abstract idea ''similar to other 'fundamental economic concepts' found to be abstract ideas by the Supreme Court and this court''); *buySAFE, Inc.* v. *Google, Inc.,* 765 F.3d. 1350, 1355 (Fed. Cir. 2014) (holding that concept of ''creating a contractual relationship—a 'transaction performance guaranty' '' is an abstract idea); *In re Comiskey,* 554 F.3d 967, 981 (Fed. Cir. 2009) (claims directed to ''resolving a legal dispute between two parties by the decision of a human arbitrator'' are ineligible); *Ultramercial, Inc.* v. *Hulu,* LLC, 772 F.3d 709, 715 (Fed Cir. 2014) (holding that claim ''describe[ing] only the abstract idea of showing an advertisement before delivering free content'' is patent ineligible); *In re Ferguson,* 558 F.3d 1359, 1364 (Fed Cir. 2009) (holding methods ''directed to organizing business or legal relationships in the structuring of a sales force (or marketing company)'' to be ineligible); *Credit Acceptance,* 859 F.3d 1044 at 1054 (''The Board determined that the claims are directed to the abstract idea of 'processing an application for financing a purchase.' . . . We agree.''); *Interval Licensing,* 896 F.3d at 1344–45 (concluding that ''[s]tanding alone, the act of providing someone an additional set of information without disrupting the ongoing provision of an initial set of information is an abstract idea,'' observing that the district court ''pointed to the nontechnical human activity of passing a note to a person who is in the middle of a meeting or conversation as further illustrating the basic, longstanding practice that is the focus of the [patent ineligible] claimed invention.''); *Voter Verified, Inc.* v. *Election Systems & Software, LLC,* 887 F.3d 1376, 1385 (Fed. Cir. 2018) (finding the concept of ''voting, verifying the vote, and submitting the vote for tabulation,'' a ''fundamental activity'' that humans have performed for hundreds of years, to be an abstract idea); *In re Smith,* 815 F.3d 816, 818 (Fed. Cir. 2016) (concluding that ''[a]pplicants' claims, directed to rules for conducting a wagering game'' are abstract).

[14] If a claim, under its broadest reasonable interpretation, covers performance in the mind but for the recitation of generic computer components, then it is still in the mental processes category unless the claim cannot practically be performed in the mind. *See Intellectual Ventures I LLC* v. *Symantec Corp.,* 838 F.3d 1307, 1318 (Fed. Cir. 2016) (''[W]ith the exception of generic computer-implemented steps, there is nothing in the claims themselves that foreclose them from being performed by a human, mentally or with pen and paper.''); *Mortg. Grader, Inc.* v. *First Choice Loan Servs. Inc.,* 811 F.3d. 1314, 1324 (Fed. Cir. 2016) (holding that computer-implemented method for ''anonymous loan shopping'' was an abstract idea because it could be ''performed by humans without a computer''); *Versata Dev. Grp.* v. *SAP Am., Inc.,* 793 F.3d 1306, 1335 (Fed. Cir. 2015) (''Courts have examined claims that required the use of a computer and still found that the underlying, patent-ineligible invention could be performed via pen and paper or in a person's mind.''); *CyberSource Corp.* v. *Retail Decisions, Inc.,* 654 F.3d 1366, 1375, 1372 (Fed. Cir. 2011) (holding that the incidental use of ''computer'' or ''computer readable medium'' does not make a claim otherwise directed to process that ''can be performed in the human mind, or by a human using a pen and paper'' patent eligible); *id.* at 1376 (distinguishing *Research Corp. Techs.* v. *Microsoft Corp.,* 627 F.3d 859 (Fed. Cir. 2010), and *SiRF Tech., Inc.* v. *Int'l Trade Comm'n,* 601 F.3d 1319 (Fed. Cir. 2010), as directed to inventions that ''could not, as a practical matter, be performed entirely in a human's mind''). Likewise, performance of a claim limitation using generic computer components does not necessarily preclude the claim limitation from being in the mathematical concepts grouping, *Benson,* 409 U.S. at 67, or the certain methods of organizing human activity grouping, *Alice,* 573 U.S. at 219–20.

[15] *Mayo,* 566 U.S. at 71 (''[M]ental processes[ ] and abstract intellectual concepts are not patentable, as they are the basic tools of scientific and technological work' '' (quoting *Benson,* 409 U.S. at 67)); *Flook,* 437 U.S. at 589 (same); *Benson,* 409 U.S. at 67, 65 (noting that the claimed ''conversion of [binary-coded decimal] numerals to pure binary numerals can be done mentally,'' *i.e.,* ''as a person

Claims that do not recite matter that falls within these enumerated groupings of abstract ideas should not be treated as reciting abstract ideas, except as follows: In the rare circumstance in which a USPTO employee believes a claim limitation that does not fall within the enumerated groupings of abstract ideas should nonetheless be treated as reciting an abstract idea, the procedure described in Section III.C for analyzing the claim should be followed.

II. ''Directed To'' a Judicial Exception

The Supreme Court has long distinguished between principles themselves (which are not patent eligible) and the integration of those principles into practical applications (which are patent eligible).[16] Similarly, in a growing body of decisions, the Federal Circuit has distinguished between claims that are ''directed to'' a judicial exception (which require further analysis to determine their eligibility) and those that are not (which are therefore patent eligible).[17] For example, an improvement in the functioning of a computer or other technology or technological field may render a claim patent eligible at step one of the *Alice/Mayo* test even if it recites an abstract idea, law of nature, or natural phenomenon.[18] Moreover, recent Federal Circuit jurisprudence has indicated that eligible subject matter can often be identified either at the first or the second step of the *Alice/Mayo* test.[19] These revised patent examination procedures are designed to more accurately and consistently identify claims that recite a practical application of a judicial exception (and thus are not ''directed to'' a judicial exception), thereby increasing predictability and consistency in the patent eligibility analysis. This analysis is performed at USPTO Step 2A, and incorporates certain considerations that have been applied by the courts at step one and at step two of the *Alice/Mayo* framework, given the recognized overlap in the steps depending on the facts of any given case.

In accordance with judicial precedent, and to increase consistency in examination practice, the 2019 Revised Patent Subject Matter Eligibility Guidance sets forth a procedure to determine whether a claim is ''directed to'' a judicial exception under USPTO Step 2A. Under the procedure, if a claim recites a judicial exception (a law of nature, a natural phenomenon, or an abstract idea as grouped in Section I, above), it must then be analyzed to determine whether the recited judicial exception is integrated into a practical application of that exception. A claim is not ''directed to'' a judicial exception, and thus is patent eligible, if the claim as a whole integrates the recited judicial exception into a practical application of that exception. A claim that integrates a judicial exception into a practical application will apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception.

III. Instructions for Applying Revised Step 2A During Examination

Examiners should determine whether a claim satisfies the criteria for subject matter eligibility by evaluating the claim in accordance with the criteria discussed in MPEP 2106, *i.e.,* whether the claim is to a statutory category (Step 1) and the *Alice/Mayo* test for judicial exceptions (Steps 2A and 2B). The procedure set forth herein (referred to as ''revised Step 2A'') changes how examiners should apply the first step of the *Alice/Mayo* test, which determines whether a claim is ''directed to'' a judicial exception.

As before, Step 1 of the USPTO's eligibility analysis entails considering whether the claimed subject matter falls within the four statutory categories of

would do it by head and hand.''); *Synopsys, Inc.* v. *Mentor Graphics Corp.,* 839 F.3d 1138, 1139, (Fed. Cir. 2016) (holding that claims to the mental process of ''translating a functional description of a logic circuit into a hardware component description of the logic circuit'' are directed to an abstract idea, because the claims ''read on an individual performing the claimed steps mentally or with pencil and paper''); *Mortg. Grader,* 811 F.3d. at 1324 (concluding that concept of ''anonymous loan shopping'' is an abstract idea because it could be ''performed by humans without a computer''); *In re BRCA1 & BRCA2-Based Hereditary Cancer Test Patent Litig.,* 774 F.3d 755, 763 (Fed. Cir. 2014) (concluding that concept of ''comparing BRCA sequences and determining the existence of alterations'' is an ''abstract mental process''); *In re Brown,* 645 F. App'x. 1014, 1017 (Fed. Cir. 2016) (non-precedential) (claim limitations ''encompass the mere idea of applying different known hair styles to balance one's head. Identifying head shape and applying hair designs accordingly is an abstract idea capable, as the Board notes, of being performed entirely in one's mind'').

[16] *See, e.g., Alice,* 573 U.S. at 217 (explaining that ''in applying the § 101 exception, we must distinguish between patents that claim the 'buildin[g] block[s]' of human ingenuity and those that integrate the building blocks into something more'' (quoting *Mayo,* 566 U.S. at 89) and stating that *Mayo* ''set forth a framework for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts''); *Mayo,* 566 U.S. at 80, 84 (noting that the Court in *Diehr* found ''the overall process patent eligible because of the way the additional steps of the process integrated the equation into the process as a whole,'' but the Court in *Benson* ''held that simply implementing a mathematical principle on a physical machine, namely a computer, was not a patentable application of that principle''); *Bilski,* 561 U.S. at 611 (''*Diehr* explained that while an abstract idea, law of nature, or mathematical formula could not be patented, 'an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection.' '' (quoting *Diehr,* 450 U.S. at 187) (emphasis in original)); *Diehr,* 450 U.S. at 187, 192 n.14 (explaining that the process in *Flook* was ineligible not because it contained a mathematical formula, but because it did not provide an application of the formula); *Mackay Radio,* 306 U.S. at 94 (''While a scientific truth, or the mathematical expression of it, is not patentable invention, a novel and useful structure created with the aid of knowledge of scientific truth may be.''); *Le Roy* v. *Tatham,* 55 U.S. (14 How.) 156, 175 (1852) (''The elements of the [natural phenomena] exist; the invention is not in discovering them, but in applying them to useful objects.'').

[17] *See, e.g.,* MPEP 2106.06(b) (summarizing *Enfish, McRO,* and other cases that were eligible as improvements to technology or computer functionality instead of abstract ideas); USPTO *Finjan* Memorandum (discussing *Finjan,* and *Core Wireless*); USPTO Memorandum of June 7, 2018, ''Recent Subject Matter Eligibility Decision: *Vanda Pharmaceuticals Inc.* v. *West-Ward Pharmaceuticals,*'' *available at https://www.uspto.gov/sites/default/files/documents/memo-vanda-20180607.PDF* [hereinafter ''USPTO *Vanda* Memorandum'']; *BASCOM Glob. Internet Servs., Inc.* v. *AT&T Mobility LLC,* 827 F.3d 1341, 1352 (Fed. Cir. 2016) (concluding that claims could be eligible if ordered combination of limitations ''transform the abstract idea . . . into a particular, practical application of that abstract idea.''); *Arrhythmia Research Tech., Inc.* v. *Corazonix Corp.,* 958 F.2d 1053, 1056–57 (Fed. Cir. 1992) (''As the jurisprudence developed, inventions that were implemented by the mathematically-directed performance of computers were viewed in the context of the practical application to which the computer-generated data were put.''); *CLS Bank Int'l* v. *Alice Corp. Pty. Ltd.,* 717 F.3d 1269, 1315 (Fed. Cir. 2013) (Moore, J., joined by Rader, C.J., and Linn and O'Malley, JJ., dissenting in part) (''The key question is thus whether a claim recites a sufficiently concrete and practical application of an abstract idea to qualify as patent-eligible.''), *aff'd,* 573 U.S. 208 (2014).

[18] *See, e.g., McRO,* 837 F.3d at 1316; *Enfish,* 822 F.3d at 1336; *Core Wireless,* 880 F.3d at 1362.

[19] *See, e.g., Vanda Pharm. Inc.* v. *West-Ward Pharm. Int'l Ltd.,* 887 F.3d 1117, 1134 (Fed. Cir. 2018) (''If the claims are not directed to a patent ineligible concept at step one, we need not address step two of the inquiry.''); *Rapid Litig. Mgmt. Ltd.* v. *CellzDirect, Inc.,* 827 F.3d 1042, 1050 (Fed. Cir. 2016) (holding that claimed invention is patent eligible because it is not directed to a patent-ineligible concept under step one or is an inventive application of the patent-ineligible concept under step two); *Enfish,* 822 F.3d at 1339 (noting that eligibility determination can be reached either because claims not directed to an abstract idea under step one or recite a concrete improvement under step two); *McRO,* 837 F.3d at 1313 (recognizing that the ''court must look to the claims as an ordered combination'' in determining patentability ''[w]hether at step one or step two of the *Alice* test''); *Amdocs,* 841 F.3d at 1294 (observing that recent cases ''suggest that there is considerable overlap between step one and step two, and in some situations [the inventive concept] analysis could be accomplished without going beyond step one''). *See also Ancora Techs.* v. *HTC Am.,* 908 F.3d 1343, 1349 (Fed. Cir. 2018) (noting, in accord with the ''recognition of overlaps between some step one and step two considerations,'' that its conclusion of eligibility at step one is ''indirectly reinforced by some of [its] prior holdings under step two'').

patentable subject matter identified by 35 U.S.C. 101: Process, machine, manufacture, or composition of matter. The 2019 Revised Patent Subject Matter Eligibility Guidance does not change Step 1 or the streamlined analysis, which are discussed in MPEP 2106.03 and 2106.06, respectively. Examiners may continue to use a streamlined analysis (Pathway A) when the patent eligibility of a claim is self-evident.

Step 2A of the 2019 Revised Patent Subject Matter Eligibility Guidance is a two-prong inquiry. In Prong One, examiners evaluate whether the claim recites a judicial exception.[20] This prong is similar to procedures in prior guidance except that when determining if a claim recites an abstract idea, examiners now refer to the subject matter groupings of abstract ideas in Section I instead of comparing the claimed concept to the USPTO's prior ''Eligibility Quick Reference Sheet Identifying Abstract Ideas.''

- If the claim recites a judicial exception (*i.e.,* an abstract idea enumerated in Section I of the 2019 Revised Patent Subject Matter Eligibility Guidance, a law of nature, or a natural phenomenon), the claim requires further analysis in Prong Two.
- If the claim does not recite a judicial exception (a law of nature, natural phenomenon, or subject matter within the enumerated groupings of abstract ideas in Section I), then the claim is eligible at Prong One of revised Step 2A. This concludes the eligibility analysis, except in the rare circumstance described below.[21]
- In the rare circumstance in which an examiner believes a claim limitation that does not fall within the enumerated groupings of abstract ideas should nonetheless be treated as reciting an abstract idea, the procedure described in Section III.C for analyzing the claim should be followed.

In Prong Two, examiners evaluate whether the claim recites additional elements that integrate the exception into a practical application of that exception. This prong adds a more detailed eligibility analysis to step one of the *Alice/Mayo* test (USPTO Step 2A) than was required under prior guidance.

- If the recited exception is integrated into a practical application of the exception, then the claim is eligible at Prong Two of revised Step 2A. This concludes the eligibility analysis.
- If, however, the additional elements do not integrate the exception into a practical application, then the claim is directed to the recited judicial exception, and requires further analysis under Step 2B (where it may still be eligible if it amounts to an ''inventive concept'').[22]

The following discussion provides additional detail on this revised procedure.

A. Revised Step 2A

1. Prong One: Evaluate Whether the Claim Recites a Judicial Exception

In Prong One, examiners should evaluate whether the claim recites a judicial exception, *i.e.,* an abstract idea, a law of nature, or a natural phenomenon. If the claim does not recite a judicial exception, it is not directed to a judicial exception (Step 2A: NO) and is eligible. This concludes the eligibility analysis. If the claim does recite a judicial exception, then it requires further analysis in Prong Two of Revised Step 2A to determine whether it is directed to the recited exception, as explained in Section III.A.2 of the 2019 Revised Patent Subject Matter Eligibility Guidance.

For abstract ideas, Prong One represents a change as compared to prior guidance. To determine whether a claim recites an abstract idea in Prong One, examiners are now to: (a) Identify the specific limitation(s) in the claim under examination (individually or in combination) that the examiner believes recites an abstract idea; and (b) determine whether the identified limitation(s) falls within the subject matter groupings of abstract ideas enumerated in Section I of the 2019 Revised Patent Subject Matter Eligibility Guidance. If the identified limitation(s) falls within the subject matter groupings of abstract ideas enumerated in Section I, analysis should proceed to Prong Two in order to evaluate whether the claim integrates the abstract idea into a practical application. When evaluating Prong One, examiners are no longer to use the USPTO's ''Eligibility Quick Reference Sheet Identifying Abstract Ideas,'' which has been superseded by this document.

In the rare circumstance in which an examiner believes a claim limitation that does not fall within the enumerated groupings of abstract ideas should nonetheless be treated as reciting an abstract idea, the procedure described in Section III.C for analyzing the claim should be followed.

For laws of nature and natural phenomena, Prong One does not represent a change. Examiners should continue to follow existing guidance to identify whether a claim recites one of these exceptions,[23] and if it does, proceed to Prong Two of the 2019 Revised Patent Subject Matter Eligibility Guidance in order to evaluate whether the claim integrates the law of nature or natural phenomenon into a practical application.

2. Prong Two: If the Claim Recites a Judicial Exception, Evaluate Whether the Judicial Exception Is Integrated Into a Practical Application

In Prong Two, examiners should evaluate whether the claim as a whole integrates the recited judicial exception into a practical application of the exception. A claim that integrates a judicial exception into a practical application will apply, rely on, or use the judicial exception in a manner that imposes a meaningful limit on the judicial exception, such that the claim is more than a drafting effort designed to monopolize the judicial exception. When the exception is so integrated, then the claim is not directed to a judicial exception (Step 2A: NO) and is eligible. This concludes the eligibility analysis. If the additional elements do not integrate the exception into a practical application, then the claim is directed to the judicial exception (Step 2A: YES), and requires further analysis under Step 2B (where it may still be eligible if it amounts to an inventive concept), as explained in Section III.B of the 2019 Revised Patent Subject Matter Eligibility Guidance.

Prong Two represents a change from prior guidance. The analysis under Prong Two is the same for all claims reciting a judicial exception, whether the exception is an abstract idea, a law of nature, or a natural phenomenon.

Examiners evaluate integration into a practical application by: (a) Identifying whether there are any additional elements recited in the claim beyond

[20] This notice does not change the type of claim limitations that are considered to recite a law of nature or natural phenomenon. For more information about laws of nature and natural phenomena, including products of nature, see MPEP 2106.04(b) and (c).

[21] Even if a claim is determined to be patent eligible under section 101, this or any other step of the eligibility analysis does not end the inquiry. The claims must also satisfy the other conditions and requirements for patentability, for example, under section 102 (novelty), 103 (nonobviousness), or 112 (enablement, written description, definiteness). *Bilski,* 561 U.S. at 602. Examiners should take care not to confuse or intermingle patentability requirements of these separate sections with patent eligibility analysis under section 101.

[22] *See, e.g., Amdocs,* 841 F.3d at 1300, 1303; *BASCOM,* 827 F.3d at 1349–52; *DDR Holdings, LLC* v. *Hotels.com,* L.P., 773 F.3d 1245, 1257–59 (Fed. Cir. 2014); USPTO *Berkheimer* Memorandum; *see also Rapid Litig.,* 827 F.3d at 1050 (holding that claimed invention is patent eligible because it is not directed to a patent-ineligible concept under step one or is an inventive application of the patent-ineligible concept under step two).

[23] *See* MPEP 2106.04(b)–(c).

the judicial exception(s); and (b) evaluating those additional elements individually and in combination to determine whether they integrate the exception into a practical application, using one or more of the considerations laid out by the Supreme Court and the Federal Circuit, for example those listed below. While some of the considerations listed below were discussed in prior guidance in the context of Step 2B, evaluating them in revised Step 2A promotes early and efficient resolution of patent eligibility, and increases certainty and reliability. Examiners should note, however, that revised Step 2A specifically excludes consideration of whether the additional elements represent well-understood, routine, conventional activity. Instead, analysis of well-understood, routine, conventional activity is done in Step 2B. Accordingly, in revised Step 2A examiners should ensure that they give weight to all additional elements, whether or not they are conventional, when evaluating whether a judicial exception has been integrated into a practical application.

In the context of revised Step 2A, the following exemplary considerations are indicative that an additional element (or combination of elements) [24] may have integrated the exception into a practical application:

- An additional element reflects an improvement in the functioning of a computer, or an improvement to other technology or technical field; [25]
- an additional element that applies or uses a judicial exception to effect a particular treatment or prophylaxis for a disease or medical condition; [26]
- an additional element implements a judicial exception with, or uses a judicial exception in conjunction with, a particular machine or manufacture that is integral to the claim; [27]
- an additional element effects a transformation or reduction of a particular article to a different state or thing; [28] and
- an additional element applies or uses the judicial exception in some other meaningful way beyond generally linking the use of the judicial exception to a particular technological environment, such that the claim as a whole is more than a drafting effort designed to monopolize the exception.[29]

This is not an exclusive list, and there may be other examples of integrating the exception into a practical application.

The courts have also identified examples in which a judicial exception has not been integrated into a practical application:

- An additional element merely recites the words ''apply it'' (or an equivalent) with the judicial exception, or merely includes instructions to implement an abstract idea on a computer, or merely uses a computer as a tool to perform an abstract idea; [30]
- an additional element adds insignificant extra-solution activity to the judicial exception; [31] and
- an additional element does no more than generally link the use of a judicial exception to a particular technological environment or field of use.[32]

It is critical that examiners consider the claim as a whole when evaluating whether the judicial exception is meaningfully limited by integration into a practical application of the exception. Some elements may be enough on their own to meaningfully limit an exception, but other times it is the combination of elements that provide the practical application. When evaluating whether an element (or combination of elements) integrates an exception into a practical application, examiners should give careful consideration to both the element and how it is used or arranged in the claim as a whole. Because revised Step 2A does not evaluate whether an additional element is well-understood, routine, conventional activity, examiners are reminded that a claim that includes conventional elements may still integrate an exception into a practical application, thereby satisfying the subject matter eligibility requirement of Section 101.[33]

---

[24] USPTO guidance uses the term ''additional elements'' to refer to claim features, limitations, and/or steps that are recited in the claim beyond the identified judicial exception. Again, whether an additional element or combination of elements integrate the exception into a practical application should be evaluated on the claim as a whole.

[25] For example, a modification of internet hyperlink protocol to dynamically produce a dual-source hybrid web page. See MPEP 2106.05(a) for more information concerning improvements in the functioning of a computer or to any other technology or technical field, including a discussion of the exemplar provided herein, which is based on *DDR Holdings,* 773 F.3d at 1258–59. See also USPTO *Finjan* Memorandum (discussing *Finjan* and *Core Wireless*).

[26] For example, an immunization step that integrates an abstract idea into a specific process of immunizing that lowers the risk that immunized patients will later develop chronic immune-mediated diseases. *See, e.g., Classen Immunotherapies, Inc.* v. *Biogen IDEC,* 659 F.3d 1057, 1066–68 (Fed. Cir. 2011). *See also Vanda Pharm. Inc.* v. *West-Ward Pharm. Int'l Ltd.,* 887 F.3d 1117, 1135 (Fed. Cir. 2018) (holding claims to the practical application of the natural relationships between iloperidone, CYP2D6 metabolism, and QTc prolongation to treat schizophrenia, not merely the recognition of those relationships, to be patent eligible at *Mayo/Alice* step 1 (USPTO Step 2A)), and USPTO *Vanda* Memorandum (discussing *Vanda*).

[27] For example, a Fourdrinier machine (which is understood in the art to have a specific structure comprising a headbox, a paper-making wire, and a series of rolls) that is arranged in a particular way that uses gravity to optimize the speed of the machine while maintaining quality of the formed paper web. See MPEP 2106.05(b) for more information concerning use of a judicial exception with, or in conjunction with, a particular machine or manufacture, including a discussion of the exemplar provided herein, which is based on *Eibel Process Co.* v. *Minnesota & Ontario Paper Co.,* 261 U.S. 45, 64–65 (1923).

[28] For example, a process that transforms raw, uncured synthetic rubber into precision-molded synthetic rubber products by using a mathematical formula to control operation of the mold. See MPEP 2106.05(c) for more information concerning transformation or reduction of a particular article to a different state or thing, including a discussion of the exemplar provided herein, which is based on *Diehr,* 450 U.S. at 184.

[29] For example, a combination of steps including installing rubber in a press, closing the mold, constantly measuring the temperature in the mold, and automatically opening the press at the proper time, all of which together meaningfully limited the use of a mathematical equation to a practical application of molding rubber products. See MPEP 2106.05(e) for more information on this consideration, including a discussion of the exemplar provided herein, which is based on *Diehr,* 450 U.S. at 184, 187. See also USPTO *Finjan* Memorandum (discussing *Finjan* and *Core Wireless*).

[30] For example, a limitation indicating that a particular function such as creating and maintaining electronic records is performed by a computer, without specifying how. See MPEP 2106.05(f) for more information concerning mere instructions to apply a judicial exception, including a discussion of the exemplar provided herein, which is based on *Alice,* 573 U.S. at 222–26. *See also Benson,* 409 U.S. 63 (holding that merely implementing a mathematical principle on a general purpose computer is a patent ineligible abstract idea); *Credit Acceptance Corp.* v. *Westlake Services,* 859 F.3d 1044 (Fed. Cir. 2017) (using a computer as a tool to process an application for financing a purchase).

[31] For example, a mere data gathering such as a step of obtaining information about credit card transactions so that the information can be analyzed in order to detect whether the transactions were fraudulent. See MPEP 2106.05(g) for more information concerning insignificant extra-solution activity, including a discussion of the exemplar provided herein, which is based on *CyberSource,* 654 F.3d at 1375. *See also Mayo,* 566 U.S. at 79 (concluding that additional element of measuring metabolites of a drug administered to a patient was insignificant extra-solution activity, which was insufficient to confer patent eligibility); *Flook,* 437 U.S. at 590 (step of adjusting an alarm limit based on the output of a mathematical formula was ''post-solution activity'' and did not render method patent eligible).

[32] For example, a claim describing how the abstract idea of hedging could be used in the commodities and energy markets, or a claim limiting the use of a mathematical formula to the petrochemical and oil-refining fields. See MPEP 2106.05(h) concerning generally linking use of a judicial exception to a particular technological environment or field of use, including a discussion of the exemplars provided herein, which are based on *Bilski,* 561 U.S. at 612, and *Flook,* 437 U.S. at 588–90. Thus, the mere application of an abstract method of organizing human activity in a particular field is not sufficient to integrate the judicial exception into a practical application.

[33] Of course, such claims must also satisfy the other conditions and requirements of patentability, for example, under section 102 (novelty), 103 (nonobviousness), and 112 (enablement, written description, definiteness). *Bilski,* 561 U.S. at 602.

B. Step 2B: If the Claim Is Directed to a Judicial Exception, Evaluate Whether the Claim Provides an Inventive Concept

It is possible that a claim that does not ''integrate'' a recited judicial exception is nonetheless patent eligible. For example the claim may recite additional elements that render the claim patent eligible even though a judicial exception is recited in a separate claim element.[34] Along these lines, the Federal Circuit has held claims eligible at the second step of the *Alice/Mayo* test (USPTO Step 2B) because the additional elements recited in the claims provided ''significantly more'' than the recited judicial exception (*e.g.,* because the additional elements were unconventional in combination).[35] Therefore, if a claim has been determined to be directed to a judicial exception under revised Step 2A, examiners should then evaluate the additional elements individually and in combination under Step 2B to determine whether they provide an inventive concept (*i.e.,* whether the additional elements amount to significantly more than the exception itself). If the examiner determines that the element (or combination of elements) amounts to significantly more than the exception itself (Step 2B: YES), the claim is eligible, thereby concluding the eligibility analysis. If the examiner determines that the element and combination of elements does not amount to significantly more than the exception itself, the claim is ineligible (Step 2B: NO) and the examiner should reject the claim for lack of subject matter eligibility.

While many considerations in Step 2A need not be reevaluated in Step 2B, examiners should continue to consider in Step 2B whether an additional element or combination of elements:

- Adds a specific limitation or combination of limitations that are not well-understood, routine, conventional activity in the field, which is indicative that an inventive concept may be present; or
- simply appends well-understood, routine, conventional activities previously known to the industry, specified at a high level of generality, to the judicial exception, which is indicative that an inventive concept may not be present.[36]

For this reason, if an examiner had previously concluded under revised Step 2A that, *e.g.,* an additional element was insignificant extra-solution activity, they should reevaluate that conclusion in Step 2B. If such reevaluation indicates that the element is unconventional or otherwise more than what is well-understood, routine, conventional activity in the field, this finding may indicate that an inventive concept is present and that the claim is thus eligible.[37] For example, when evaluating a claim reciting an abstract idea such as a mathematical equation and a series of data gathering steps that collect a necessary input for the equation, an examiner might consider the data gathering steps to be insignificant extra-solution activity in revised Step 2A, and therefore find that the judicial exception is not integrated into a practical application.[38] However, when the examiner reconsiders the data gathering steps in Step 2B, the examiner could determine that the combination of steps gather data in an unconventional way and therefore include an ''inventive concept,'' rendering the claim eligible at Step 2B.[39] Likewise, a claim that does not meaningfully integrate a judicial exception into a practical application of the exception sufficient to pass muster at Step 2A, may nonetheless include additional subject matter that is unconventional and thus an ''inventive concept'' at Step 2B.[40]

C. Treating a Claim Limitation That Does Not Fall Within the Enumerated Groupings of Abstract Ideas as Reciting an Abstract Idea

In the rare circumstance in which an examiner believes a claim limitation that does not fall within the enumerated groupings of abstract ideas should

[34] *See, e.g., Diehr,* 450 U.S. at 187 (''Our earlier opinions lend support to our present conclusion that a claim drawn to subject matter otherwise statutory does not become nonstatutory simply because it uses a mathematical formula, computer program, or digital computer.''); *id.* at 185 (''Our conclusion regarding respondents' claims is not altered by the fact that in several steps of the process a mathematical equation and a programmed digital computer are used.'').

[35] *See, e.g., Amdocs,* 841 F.3d at 1300, 1303; *BASCOM,* 827 F.3d at 1349–52; *DDR Holdings,* 773 F.3d at 1257–59.

[36] In accordance with existing guidance, an examiner's conclusion that an additional element (or combination of elements) is well understood, routine, conventional activity must be supported with a factual determination. For more information concerning evaluation of well-understood, routine, conventional activity, see MPEP 2106.05(d), as modified by the USPTO *Berkheimer* Memorandum.

[37] *Mayo,* 566 U.S. at 82 (''[S]imply appending conventional steps, specified at a high level of generality, to laws of nature, natural phenomena, and abstract ideas cannot make those laws, phenomena, and ideas patentable.''); *but see id.* at 85 (''[T]he claimed process included not only a law of nature but also several unconventional steps (such as inserting the receptacle, applying heat to the receptacle externally, and blowing the air into the furnace) that confined the claims to a particular, useful application of the principle.'' (discussing the old English case, *Neilson* v. *Harford,* Webster's Patent Cases 295 (1841))).

[38] *See supra* note 34; *see also OIP Techs.,* 788 F.3d at 1363 (finding that gathering statistics generated based on customer testing for input to a pricing calculation ''fail[s] to 'transform' the claimed abstract idea into a patent-eligible invention'').

[39] *Compare Flook,* 437 U.S. at 585–86 (holding claimed method of updating alarm limits to be ineligible because: ''In essence, the method consists of three steps: an initial step which merely measures the present value of the process variable (*e.g.,* the temperature); an intermediate step which uses an algorithm to calculate an updated alarm-limit value; and a final step in which the actual alarm limit is adjusted to the updated value. The only difference between the conventional methods of changing alarm limits and that described in respondent's application rests in the second step—the mathematical algorithm or formula.''); *with Exergen Corp.* v. *Kaz USA, Inc.,* 725 F. App'x 959, 966 (Fed. Cir. 2018) (holding claimed body temperature detector to be eligible because: ''Here, the patent is directed to the measurement of a natural phenomenon (core body temperature). Even if the concept of such measurement is directed to a natural phenomenon and is abstract at step one, the measurement method here was not conventional, routine, and well-understood. Following years and millions of dollars of testing and development, the inventor determined for the first time the coefficient representing the relationship between temporal-arterial temperature and core body temperature and incorporated that discovery into an unconventional method of temperature measurement.'').

[40] *Compare Berkheimer,* 881 F.3d at 1370 (holding independent claim 1 to be ineligible at *Alice* step 2: ''The[ ] conventional limitations of claim 1, combined with limitations of analyzing and comparing data and reconciling differences between the data, fail to transform the abstract idea into a patent-eligible invention. The limitations amount to no more than performing the abstract idea of parsing and comparing data with conventional computer components'') (internal quotation marks and citation omitted); *with id.* (concluding that dependent claims 4–7 may be eligible: ''Claims 4–7, in contrast, contain limitations directed to the arguably unconventional inventive concept described in the specification. Claim 4 recites 'storing a reconciled object structure in the archive without substantial redundancy.' The specification states that storing object structures in the archive without substantial redundancy improves system operating efficiency and reduces storage costs. It also states that known asset management systems did not archive documents in this manner. Claim 5 depends on claim 4 and further recites 'selectively editing an object structure, linked to other structures to thereby effect a one-to-many change in a plurality of archived items.' The specification states one-to-many editing substantially reduces effort needed to update files because a single edit can update every document in the archive linked to that object structure. This one-to-many functionality is more than 'editing data in a straightforward copy-and-paste fashion,' as characterized by the district court. According to the specification, conventional digital asset management systems cannot perform one-to-many editing because they store documents with numerous instances of redundant elements, rather than eliminate redundancies through the storage of linked object structures. Claims 6–7 depend from claim 5 and accordingly contain the same limitations. These claims recite a specific method of archiving that, according to the specification, provides benefits that improve computer functionality. . . . [T]here is at least a genuine issue of material fact in light of the specification regarding whether claims 4–7 archive documents in an inventive manner that improves these aspects of the disclosed archival system.'') (internal quotation marks and citations omitted).

nonetheless be treated as reciting an abstract idea (''tentative abstract idea''), the examiner should evaluate whether the claim as a whole integrates the recited tentative abstract idea into a practical application as explained in Section III.A.2. If the claim as a whole integrates the recited tentative abstract idea into a practical application, the claim is not directed to a judicial exception (Step 2A: NO) and is eligible (thus concluding the eligibility analysis). If the claim as a whole does not integrate the recited tentative abstract idea into a practical application, then the examiner should evaluate the additional elements individually and in combination to determine whether they provide an inventive concept as explained in Section III.B. If an additional element or combination of additional elements provides an inventive concept as explained in Section III.B (Step 2B: YES), the claim is eligible (thus concluding the eligibility analysis). If the additional element or combination of additional elements does not provide an inventive concept as explained in Section III.B (Step 2B: NO), the examiner should bring the application to the attention of the Technology Center Director. Any rejection in which a claim limitation, which does not fall within the enumerated abstract ideas (tentative abstract idea), is nonetheless treated as reciting an abstract idea must be approved by the Technology Center Director (which approval will be indicated in the file record of the application), and must provide a justification [41] for why such claim limitation is being treated as reciting an abstract idea.[42]

D. Compact Prosecution

Regardless of whether a rejection under 35 U.S.C. 101 is made, a complete examination should be made for every claim under each of the other patentability requirements: 35 U.S.C. 102, 103, 112, and 101 (utility, inventorship and double patenting) and non-statutory double patenting.[43] Compact prosecution, however, does not mandate that the patentability requirements be analyzed in any particular order.

Dated: December 20, 2018.

Andrei Iancu,

Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office.

[FR Doc. 2018–28282 Filed 1–4–19; 8:45 am]

BILLING CODE 3510–16–P

[41] Such justification may include, for example, an explanation of why the element contains subject matter that, per se, invokes eligibility concerns similar to those expressed by the Supreme Court with regard to the judicial exceptions. *See supra* note 5.

[42] Similarly, in the rare circumstance in which a panel of administrative patent judges (or panel majority) believes that a claim reciting a tentative abstract idea should be treated as reciting an abstract idea, the matter should be brought to the attention of the PTAB leadership by a written request for clearance.

[43] *See* MPEP 2103 *et seq.* and 2106(III).

DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

[Docket No. PTO–P–2018–0059]

Examining Computer-Implemented Functional Claim Limitations for Compliance With 35 U.S.C. 112

AGENCY: United States Patent and Trademark Office, Commerce.

ACTION: Examination guidance; request for comments.

SUMMARY: This guidance will assist United States Patent and Trademark Office (USPTO) personnel in the examination of claims in patent applications that contain functional language, particularly patent applications where functional language is used to claim computer-implemented inventions. Part I of this guidance addresses issues related to the examination of computer-implemented functional claims having means-plus-function limitations. Part II of this guidance addresses written description and enablement issues related to the examination of computer-implemented functional claims that recite only the idea of a solution or outcome to a problem but fail to recite details of how the solution or outcome is accomplished.

DATES:

Applicable Date: The Computer-Implemented Functional Claim Limitations Guidance is effective on January 7, 2019. The Computer-Implemented Functional Claim Limitations Guidance applies to all applications, and to all patents resulting from applications, filed before, on or after January 7, 2019.

Comment Deadline Date: Written comments must be received on or before March 8, 2019.

ADDRESSES: Comments must be sent by electronic mail message over the internet addressed to: *112Guidance2019@uspto.gov.*

Electronic comments submitted in plain text are preferred, but also may be submitted in ADOBE® portable document format or MICROSOFT WORD® format. Comments not submitted electronically should be submitted on paper in a format that facilitates convenient digital scanning into ADOBE® portable document format. The comments will be available for viewing via the USPTO's internet website (*http://www.uspto.gov*). Because comments will be made available for public inspection, information that the submitter does not desire to make public, such as an address or phone number, should not be included in the comments.

FOR FURTHER INFORMATION CONTACT: Nicole D. Haines, Senior Legal Advisor, at 571–272–7717 or Jeffrey R. West, Senior Legal Advisor, at 571–272–2226, both with the Office of Patent Legal Administration.

SUPPLEMENTARY INFORMATION: The patent examination process must ensure that: (1) The claims of an application have proper written description and enablement support under 35 U.S.C. 112(a) [1] in the disclosure of the application, and (2) functional limitations (*i.e.,* claim limitations that define an element in terms of the function it performs without reciting the structure, materials, or acts that perform the function) are properly treated as means (or step) plus function limitations under 35 U.S.C. 112(f), and are sufficiently definite under 35 U.S.C. 112(b), as appropriate. These requirements are particularly relevant to computer-implemented functional claims.

The U.S. Court of Appeals for the Federal Circuit (''Federal Circuit'') has recognized a problem with broad functional claiming without adequate structural support in the specification. *Williamson* v. *Citrix Online, LLC,* 792 F.3d 1339, 1349 (Fed. Cir. 2015) (en banc) (overruling the Federal Circuit's previous application of a ''strong'' presumption that claim limitations lacking the word ''means'' are not subject to § 112(f) to address the resulting ''proliferation of functional claiming untethered to [§ 112(f)] and free of the strictures set forth in the statute''); *Function Media, LLC* v. *Google, Inc.,* 708 F.3d 1310, 1319 (Fed. Cir. 2013) (' 'Section [112(f)] is intended

[1] Section 4 of the Leahy-Smith America Invents Act (AIA) designated pre-AIA 35 U.S.C. 112, ¶ ¶ 1 through 6, as 35 U.S.C. 112(a) through (f), effective as to applications filed on or after September 16, 2012. *See* Public Law 112–29, 4(c), 125 Stat. 284, 296 (2011). AIA 35 U.S.C. 112(a) and pre-AIA 35 U.S.C. 112, ¶ 1 are collectively referred to in this notice as 35 U.S.C. 112(a); AIA 35 U.S.C. 112(b) and pre-AIA 35 U.S.C. 112, ¶ 2 are collectively referred to in this notice as 35 U.S.C. 112(b); and AIA 35 U.S.C. 112(f) and pre-AIA 35 U.S.C. 112, ¶ 6 are collectively referred to in this notice as 35 U.S.C. 112(f).

The following examples should be used in conjunction with the *2019 Revised Patent Subject Matter Eligibility Guidance* (2019 PEG). The examples below are hypothetical and only intended to be illustrative of the claim analysis under the 2019 PEG. These examples should be interpreted based on the fact patterns set forth below as other fact patterns may have different eligibility outcomes. That is, it is not necessary for a claim under examination to mirror an example claim to be subject matter eligible under the 2019 PEG. All of the claims are analyzed for eligibility in accordance with their broadest reasonable interpretation.

Note that the examples herein are numbered consecutively beginning with number 37, because 36 examples were previously issued.

The examples are illustrative only of the patent-eligibility analysis under the 2019 PEG. All claims must be ultimately analyzed for compliance with every requirement for patentability, including 35 U.S.C. 102, 103, 112, and 101 (utility, inventorship and double patenting) and non-statutory double patenting. The analyses provided below do not address considerations other than subject matter eligibility under Section 101.

Example 37 – Relocation of Icons on a Graphical User Interface

Background:

Traditionally, computer users are limited in the ways in which they can organize icons on their display. Additionally, computer users may have a large number of icons on their display, making it difficult to find the icons most used. The typically available ways to organize icons are alphabetically, by file size, and by file type. If a computer user wants a non-typical arrangement of icons, the user would need to manually manipulate the icons on their display. For example, traditional software does not automatically organize icons so that the most used icons are located near the "start" or "home" icon, where they can be easily accessed. Therefore, what is needed is a method that allows for such non-traditional arrangements to be performed automatically.

Accordingly, applicant's invention addresses this issue by providing a method for rearranging icons on a graphical user interface (GUI), wherein the method moves the most used icons to a position on the GUI, specifically, closest to the "start" icon of the computer system, based on a determined amount of use. In a first preferred embodiment, the amount of use of each icon is automatically determined by a processor that tracks the number of times each icon is selected or how much memory has been allocated to the individual processes associated with each icon over a period of time (*e.g.*, day, week, month, etc.). In another embodiment, the user can choose to manually enter which icons are used most often using any of a number of ordering and/or ranking systems known to those skilled in the art.

Claim 1:

A method of rearranging icons on a graphical user interface (GUI) of a computer system, the method comprising:

receiving, via the GUI, a user selection to organize each icon based on a specific criteria, wherein the specific criteria is an amount of use of each icon;

determining, by a processor, the amount of use of each icon over a predetermined period of time; and

automatically moving the most used icons to a position on the GUI closest to the start icon of the computer system based on the determined amount of use.

Step	Analysis
1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
2A - Prong 1: Judicial Exception Recited?	**Yes**. The claim recites the limitation of determining the amount of use of each icon over a predetermined period of time. This limitation, as drafted, is a process that, under its broadest reasonable interpretation, covers performance of the limitation in the mind but for the recitation of generic computer components. That is, other than reciting "by a processor," nothing in the claim element precludes the step from practically being performed in the mind. For example, but for the "by a processor" language, the claim encompasses the user manually calculating the amount of use of each icon. The mere nominal recitation of a generic processor does not take the claim limitation out of the mental processes grouping. Thus, the claim recites a mental process.
2A - Prong 2: Integrated into a Practical Application?	**Yes**. The claim recites the combination of additional elements of receiving, via a GUI, a user selection to organize each icon based on the amount of use of each icon, a processor for performing the determining step, and automatically moving the most used icons to a position on the GUI closest to the start icon of the computer system based on the determined amount of use. The claim as a whole integrates the mental process into a practical application. Specifically, the additional elements recite a specific manner of automatically displaying icons

	to the user based on usage which provides a specific improvement over prior systems, resulting in an improved user interface for electronic devices. Thus, the claim is **eligible** because it is not directed to the recited judicial exception.
2B: Claim provides an Inventive Concept?	**N/A.**

Claim 2:

A method of rearranging icons on a graphical user interface (GUI) of a computer system, the method comprising:

receiving, via the GUI, a user selection to organize each icon based on a specific criteria, wherein the specific criteria is an amount of use of each icon;

determining the amount of use of each icon using a processor that tracks how much memory has been allocated to each application associated with each icon over a predetermined period of time; and

automatically moving the most used icons to a position on the GUI closest to the start icon of the computer system based on the determined amount of use.

Step	Analysis
1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
2A - Prong 1: Judicial Exception Recited?	**No**. The claim does not recite any of the judicial exceptions enumerated in the 2019 PEG. For instance, the claim does not recite a mental process because the claim, under its broadest reasonable interpretation, does not cover performance in the mind but for the recitation of generic computer components. For example, the "determining step" now requires action by a processor that cannot be practically applied in the mind. . In particular, the claimed step of determining the amount of use of each icon by tracking how much memory has been allocated to each application associated with each icon over a predetermined period of time is not practically performed in the human mind, at least because it requires a processor accessing computer memory indicative of application usage. Further, the claim does not recite any

	method of organizing human activity, such as a fundamental economic concept or managing interactions between people. Finally, the claim does not recite a mathematical relationship, formula, or calculation. Thus, the claim is **eligible** because it does not recite a judicial exception.
2A - Prong 2: Integrated into a Practical Application?	**N/A.**
2B: Claim provides an Inventive Concept?	**N/A.**

Claim 3:

A method of ranking icons of a computer system, the method comprising:

determining, by a processor, the amount of use of each icon over a predetermined period of time; and

ranking the icons, by the processor, based on the determined amount of use.

Step	Analysis
1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
2A - Prong 1: Judicial Exception Recited?	**Yes**. The claim recites the limitations of determining the amount of use of each icon over a predetermined period of time and ranking the icons based on the determined amount of use. The determining limitation, as drafted, is a process that, under its broadest reasonable interpretation, covers performance of the limitation in the mind but for the recitation of generic computer components. That is, other than reciting "by a processor," nothing in the claim precludes the determining step from practically being performed in the human mind. For example, but for the "by a processor" language, the claim encompasses the user manually calculating the amount of use of each icon. This limitation is a mental process. The ranking limitations, as drafted, is also a process that, under its broadest reasonable

	interpretation, covers performance of the limitation in the mind but for the recitation of generic computer components. That is, other than reciting "by a processor," nothing in the claim precludes the ranking step from practically being performed in the human mind. For example, but for the "by a processor" language, the claim encompasses the user thinking that the most-used icons should be ranked higher than the least-used icons. Thus, this limitation is also a mental process.
2A - Prong 2: Integrated into a Practical Application?	**No**. The claim recites one additional element: that a processor is used to perform both the ranking and determining steps. The processor in both steps is recited at a high level of generality, i.e., as a generic processor performing a generic computer function of processing data (the amount of use of each icon, or the ranking of the icons based on the determined amount of use). This generic processor limitation is no more than mere instructions to apply the exception using a generic computer component. Accordingly, this additional element does not integrate the abstract idea into a practical application because it does not impose any meaningful limits on practicing the abstract idea. The claim is directed to the abstract idea.
2B: Claim provides an Inventive Concept?	**No.** As discussed with respect to Step 2A Prong Two, the additional element in the claim amounts to no more than mere instructions to apply the exception using a generic computer component. The same analysis applies here in 2B, i.e., mere instructions to apply an exception using a generic computer component cannot integrate a judicial exception into a practical application at Step 2A or provide an inventive concept in Step 2B. The claim is **ineligible**.

Example 38 – Simulating an Analog Audio Mixer

Background:

Audiophiles are people interested in high-fidelity audio reproduction. For many, this means listening to music in its analog form, as digital audio files are considered to "lose" much of the sound quality in the conversion from analog to digital. Prior inventions attempted to create digital simulations of analog audio mixers to simulate the sounds from analog circuits. However, the prior art audio mixer simulations do not produce the same sound quality as the actual analog circuits.

Applicant's invention seeks to more closely replicate the sound quality of an analog audio mixer by accounting for the slight variances in analog circuit values that are generated during the circuit's manufacturing. By simulating these variances, a more authentic sound can be created that is preferential for the listener. The method begins with a model of an analog circuit representing an audio mixing console. The model includes a location of all the circuit elements within the circuit, an initial value for each of the circuit elements, and a manufacturing tolerance range for each of the circuit elements. A randomized working value of each element is then determined using a normally distributed pseudo random number generator (PRNG) based on the initial value of the circuit element and the manufacturing tolerance range. The model is then simulated using a bilinear transformation to create a digital representation of the analog circuit. This digital representation is then presented to the user through a graphical user interface as an operational digital audio mixer. The user can use the graphical user interface to test the sound quality of the digital representation. If the sound quality is not acceptable to the user, the user can generate new randomized working values for all the circuit elements and simulate another digital representation of the analog audio mixer.

Claim:

A method for providing a digital computer simulation of an analog audio mixer comprising:

initializing a model of an analog circuit in the digital computer, said model including a location, initial value, and a manufacturing tolerance range for each of the circuit elements within the analog circuit;

generating a normally distributed first random value for each circuit element, using a pseudo random number generator, based on a respective initial value and manufacturing tolerance range; and

simulating a first digital representation of the analog circuit based on the first random value and the location of each circuit element within the analog circuit.

Step	Analysis
1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
2A - Prong 1: Judicial Exception Recited?	**No.** The claim does not recite any of the judicial exceptions enumerated in the 2019 PEG. The claim does not recite a mathematical relationship, formula, or calculation. While some of the limitations may be based on mathematical concepts, the mathematical concepts are not recited in the claims. With respect to mental processes, the claim does not recite a mental process because the steps are not practically performed in the human mind. Finally, the claim does not recite a certain method of organizing human activity such as a fundamental economic concept or commercial and legal interactions. The claim is **eligible** because it does not recite a judicial exception.
2A - Prong 2: Integrated into a Practical Application?	**N/A.**
2B: Claim provides an Inventive Concept?	**N/A.**

Example 39 - Method for Training a Neural Network for Facial Detection

Background:

Facial detection is a computer technology for identifying human faces in digital images. This technology has several different potential uses, ranging from tagging pictures in social networking sites to security access control. Some prior methods use neural networks to perform facial detection. A neural network is a framework of machine learning algorithms that work together to classify inputs based on a previous training process. In facial detection, a neural network classifies images as either containing a human face or not, based upon the model being previously trained on a set of facial and non-facial images. However, these prior methods suffer from the inability to robustly detect human faces in images where there are shifts, distortions, and variations in scale and rotation of the face pattern in the image.

Applicant's invention addresses this issue by using a combination of features to more robustly detect human faces. The first feature is the use of an expanded training set of facial images to train the neural network. This expanded training set is developed by applying mathematical transformation functions on an acquired set of facial images. These transformations can include affine transformations, for example, rotating, shifting, or mirroring or filtering transformations, for example, smoothing or contrast reduction. The neural networks are then trained with this expanded training set using stochastic learning with backpropagation which is a type of machine learning algorithm that uses the gradient of a mathematical loss function to adjust the weights of the network. Unfortunately, the introduction of an expanded training set increases false positives when classifying non-facial images. Accordingly, the second feature of applicant's invention is the minimization of these false positives by performing an iterative training algorithm, in which the system is retrained with an updated training set containing the false positives produced after face detection has been performed on a set of non-facial images. This combination of features provides a robust face detection model that can detect faces in distorted images while limiting the number of false positives.

Claim:

A computer-implemented method of training a neural network for facial detection comprising:

collecting a set of digital facial images from a database;

applying one or more transformations to each digital facial image including mirroring, rotating, smoothing, or contrast reduction to create a modified set of digital facial images;

creating a first training set comprising the collected set of digital facial images, the modified set of digital facial images, and a set of digital non-facial images;

training the neural network in a first stage using the first training set;

creating a second training set for a second stage of training comprising the first training set and digital non-facial images that are incorrectly detected as facial images after the first stage of training; and

training the neural network in a second stage using the second training set.

Step	Analysis
1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
2A - Prong 1: Judicial Exception Recited?	**No**. The claim does not recite any of the judicial exceptions enumerated in the 2019 PEG. For instance, the claim does not recite any mathematical relationships, formulas, or calculations. While some of the limitations may be based on mathematical concepts, the mathematical concepts are not recited in the claims. Further, the claim does not recite a mental process because the steps are not practically performed in the human mind. Finally, the claim does not recite any method of organizing human activity such as a fundamental economic concept or managing interactions between people. Thus, the claim is **eligible** because it does not recite a judicial exception.
2A - Prong 2: Integrated into a Practical Application?	**N/A.**
2B: Claim provides an Inventive Concept?	**N/A.**

Example 40 – Adaptive Monitoring of Network Traffic Data

Background:

Network visibility tools enable close monitoring of computer network traffic, applications, performance, and resources. The data acquired through these network visibility tools is extremely useful in optimizing network performance, resolving network issues, and improving network security. One industry standard network visibility protocol is NetFlow. In a typical setup, a NetFlow exporter generates and exports network traffic statistics (in the form of NetFlow records) to at least one NetFlow collector that analyzes the statistics. Because NetFlow records are very large, the continual generation and export of NetFlow records in such a setup substantially increases the traffic volume on the network, which hinders network performance. Moreover, continual analysis of the network is not always necessary when the network is performing under normal conditions.

Applicant's invention addresses this issue by varying the amount of network data collected based on monitored events in the network. That is, the system will only collect NetFlow protocol data and export a NetFlow record when abnormal network conditions are detected. In practice, during normal network conditions, a network appliance collects network data relating to network traffic passing through the network appliance. This network data, for example, could include network delay, packet loss, or jitter. Periodically, the network data is compared to a predefined quality threshold. If this network data is greater than the predefined quality threshold, an abnormal condition is detected. When an abnormal condition is present, the system begins collecting NetFlow protocol data, which can later be used for analyzing the abnormal condition. During this time, the network appliance continues to monitor the network conditions (*i.e.*, comparing collected network data to the predetermined quality threshold) and when the abnormal condition no longer exists, NetFlow protocol data is no longer collected.

Claim 1:

A method for adaptive monitoring of traffic data through a network appliance connected between computing devices in a network, the method comprising:

collecting, by the network appliance, traffic data relating to the network traffic passing through the network appliance, the traffic data comprising at least one of network delay, packet loss, or jitter;

comparing, by the network appliance, at least one of the collected traffic data to a predefined threshold; and

collecting additional traffic data relating to the network traffic when the collected traffic data is greater than the predefined threshold, the additional traffic data comprising Netflow protocol data.

Step	Analysis
1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
2A - Prong 1: Judicial Exception Recited?	**Yes**. The claim recites the limitation of comparing at least one of the collected traffic data to a predefined threshold. This limitation, as drafted, is a process that, under its broadest reasonable interpretation, covers performance of the limitation in the mind but for the recitation of generic computer components. That is, other than reciting "by the network appliance," nothing in the claim element precludes the step from practically being performed in the mind. For example, but for the "by the network appliance" language, the claim encompasses a user simply comparing the collected packet loss data to a predetermined acceptable quality percentage in his/her mind. The mere nominal recitation of a generic network appliance does not take the claim limitation out of the mental processes grouping. Thus, the claim recites a mental process.
2A - Prong 2: Integrated into a Practical Application?	**Yes**. The claim recites the combination of additional elements of collecting at least one of network delay, packet loss, or jitter relating to the network traffic passing through the network appliance, and collecting additional Netflow protocol data relating to the network traffic when the collected network delay, packet loss, or jitter is greater than the predefined threshold. Although each of the collecting steps analyzed individually may be viewed as mere pre- or post-solution activity, the claim as a whole is directed to a particular improvement in collecting traffic data. Specifically, the method limits collection of additional Netflow protocol data to when the initially collected data reflects an abnormal condition, which avoids excess traffic volume on the network and hindrance of network performance. The collected data can then be used to analyze the cause of the abnormal condition. This provides a specific improvement over prior systems, resulting in improved network monitoring. The claim as a whole integrates the mental process into a practical application. Thus, the claim is **eligible** because it is not directed to the recited judicial exception.
2B: Claim provides an Inventive Concept?	**N/A.**

Claim 2:

A method for monitoring of traffic data through a network appliance connected between computing devices in a network, the method comprising:

collecting, by the network appliance, traffic data relating to the network traffic passing through the network appliance, the traffic data comprising at least one of network delay, packet loss, or jitter; and

comparing, by the network appliance, at least one of the collected traffic data to a predefined threshold.

Step	Analysis
1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
2A - Prong 1: Judicial Exception Recited?	**Yes**. The claim recites the limitation of comparing at least one of the collected traffic data to a predefined threshold. This limitation, as drafted, is a process that, under its broadest reasonable interpretation, covers performance of the limitation in the mind but for the recitation of generic computer components. That is, other than reciting "by the network appliance," nothing in the claim element precludes the step from practically being performed in the mind. For example, but for the "by the network appliance" language, the claim encompasses a user simply comparing the collected packet loss data to a predetermined acceptable quality percentage in his/her mind. The mere nominal recitation of a generic network appliance does not take the claim limitation out of the mental processes grouping. Thus, the claim recites a mental process.
2A - Prong 2: Integrated into a Practical Application?	**No**. The claim recites two additional elements: collecting at least one of network delay, packet loss, or jitter relating to the network traffic passing through the network appliance, and that a generic network appliance performs the comparing step. The collecting step is recited at a high level of generality (i.e., as a general means of gathering network traffic data for use in the comparison step), and amounts to mere data gathering, which is a form of insignificant extra-solution activity. The network appliance that performs the comparison step is also recited at a high level of generality, and merely automates the comparison step. Each of the additional limitations is no more than mere instructions to apply the exception using a generic computer component (the network appliance).

	The combination of these additional elements is no more than mere instructions to apply the exception using a generic computer component (the network appliance). Accordingly, even in combination, these additional elements do not integrate the abstract idea into a practical application because they do not impose any meaningful limits on practicing the abstract idea. The claim is directed to the abstract idea.
2B: Claim provides an Inventive Concept?	**No.** As discussed with respect to Step 2A Prong Two, the additional elements in the claim amount to no more than mere instructions to apply the exception using a generic computer component. The same analysis applies here in 2B, i.e., mere instructions to apply an exception on a generic computer cannot integrate a judicial exception into a practical application at Step 2A or provide an inventive concept in Step 2B. Under the 2019 PEG, a conclusion that an additional element is insignificant extra-solution activity in Step 2A should be re-evaluated in Step 2B. Here, the collecting step was considered to be extra-solution activity in Step 2A, and thus it is re-evaluated in Step 2B to determine if it is more than what is well-understood, routine, conventional activity in the field. The background of the example does not provide any indication that the network appliance is anything other than a generic, off-the-shelf computer component, and the *Symantec*, *TLI*, and *OIP Techs.* court decisions cited in MPEP 2106.05(d)(II) indicate that mere collection or receipt of data over a network is a well-understood, routine, and conventional function when it is claimed in a merely generic manner (as it is here). Accordingly, a conclusion that the collecting step is well-understood, routine, conventional activity is supported under *Berkheimer* Option 2. For these reasons, there is no inventive concept in the claim, and thus it is **ineligible**.

Example 41 – Cryptographic Communications

Background:

Security of information is of increasing importance in computer technology. It is critical that data being sent from a sender to a recipient is unable to be intercepted and understood by an intermediate source. In addition, authentication of the source of the message must be ensured along with the verification of and security of the message content. Various cryptographic encoding and decoding methods are available to assist with these security and authentication needs. However, many of them require expensive encoding and decoding hardware as well as a secure way of sharing the private key used to encrypt and decrypt the message. There is a need to perform these same security and authentication functions efficiently over a public key system so that information can be shared easily between users who do not know each other and have not shared the key used to encrypt and decrypt the information.

To solve these problems, applicants have invented a method for establishing cryptographic communications using an algorithm to encrypt a plaintext into a ciphertext. The invention includes at least one encoding device and at least one decoding device, which are computer terminals, and a communication channel, where the encoding and decoding devices are coupled to the communication channel. The encoding device is responsive to a precoded message-to-be-transmitted M and an encoding key E to provide a ciphertext word C for transmission to a particular decoding device. The message-to-be-transmitted is precoded by converting it to a numerical representation which is broken into one or more blocks M_A of equal length. This precoding may be done by any conventional means. The resulting message M_A is a number representative of a message-to-be-transmitted, where $0 \leq M_A \leq n-1$, where n is a composite number of the form $n=p*q$, where p and q are prime numbers. The encoding key E is a pair of positive integers e and n, which are related to the particular decoding device. The encoding device distinctly encodes each of the n possible messages. The transformation provided by the encoding device is described by the relation $C_A=M_A^e \pmod n$ where e is a number relatively prime to $(p-1)*(q-1)$. The encoding device transmits the ciphertext word signal C_A to the decoding device over the communications channel. The decoding device is responsive to the received ciphertext word C_A and a decoding key to transform the ciphertext to a received message word M_A'.

The invention improves upon prior methods for establishing cryptographic communications because by using only the variables n and e (which are publicly known), a plaintext can be encrypted by anyone. The variables p and q are only known by the owner of the decryption key d and are used to generate the decryption key (private key d is not claimed below). Thus, the security of the cipher relies on the difficulty of factoring large integers by computers, and there is no known efficient algorithm to recover the plaintext given the ciphertext and the public information (n, e) (assuming that p and q are sufficiently large).

Claim:

A method for establishing cryptographic communications between a first computer terminal and a second computer terminal comprising:

receiving a plaintext word signal at the first computer terminal;

transforming the plaintext word signal to one or more message block word signals M_A;

encoding each of the message block word signals M_A to produce a ciphertext word signal C_A, whereby $C_A=M_A^e \pmod n$;

where C_A is a number representative of an encoded form of message word M_A;

where M_A corresponds to a number representative of a message and $0 \leq M_A \leq n-1$;

where n is a composite number of the form n=p*q;

where p and q are prime numbers;

where e is a number relatively prime to (p-1)*(q-1); and

transmitting the ciphertext word signal C_A to the second computer terminal over a communication channel.

Step	Analysis
1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
2A - Prong 1: Judicial Exception Recited?	**Yes**. The claim recites a mathematical formula or calculation that is used to encode each of the message block word signals M_A to produce a ciphertext word signal C_A, whereby $C_A=M_A^e \pmod n$. Thus, the claim recites a mathematical concept. Note that, in this example, the "encoding" step is determined to recite a mathematical concept because the claim explicitly recites a mathematical formula or calculation.
2A - Prong 2: Integrated into a Practical Application?	**Yes**. The combination of additional elements in the claim (receiving the plaintext word signal at the first computer terminal, transforming the plaintext word signal to one or message block word signals M_A, and transmitting the encoded ciphertext word signal C_A to the second computer terminal over a communication channel) integrates the exception into a practical application. In particular, the combination of additional elements use the mathematical formulas and calculations in a specific manner that sufficiently limits the use of the mathematical concepts to the practical application of transmitting the ciphertext word signal to a computer terminal over a communication channel. Thus, the mathematical concepts are integrated into a process that secures private

	network communications, so that a ciphertext word signal can be transmitted between computers of people who do not know each other or who have not shared a private key between them in advance of the message being transmitted, where the security of the cipher relies on the difficulty of factoring large integers by computers. Thus, the claim is not directed to the recited judicial exception, and the claim is **eligible.** Note that well-understood, routine, conventional subject matter can integrate an abstract idea into a practical application. Thus, even though receiving a signal at a first computer, transforming it and transmitting the transformed signal to a second computer are described in the background as being conventional, Step 2A – Prong 2 does not evaluate whether the additional elements are conventional to determine whether the abstract idea is integrated into a practical application.
2B: Claim provides an Inventive Concept?	**N/A.**

Example 42 – Method for Transmission of Notifications When Medical Records Are Updated

Background:

Patients with chronic or undiagnosed illnesses often must visit several different medical providers for diagnosis and treatment. These physicians may be physically separate from each other and unaware of each other. During a visit, each medical provider records information about the patient's condition in their own local patient records. These records are often stored locally on a computer in a non-standard format selected by whichever hardware or software platform is in use in the medical provider's local office. It is difficult for medical providers to share updated information about a patient's condition with other health care providers using current patient management systems, due to the above challenges. This can lead to problems with managing prescriptions or having patients duplicate tests, for example. Currently, medical providers must continually monitor a patient's medical records for updated information, which is often-times incomplete since records in separate locations are not timely or readily-shared or cannot be consolidated due to format inconsistencies as well as physicians who are unaware that other physicians are also seeing the patient for varying reasons.

To solve this problem, applicant has invented a network-based patient management method that collects, converts and consolidates patient information from various physicians and health-care providers into a standardized format, stores it in network-based storage devices, and generates messages notifying health care providers or patients whenever that information is updated. The method provides a graphical user interface (GUI) by a content server, which is hardware or a combination of both hardware and software. A user, such as a health care provider or patient, is given remote access through the GUI to view or update information about a patient's medical condition using the user's own local device (e.g., a personal computer or wireless handheld device). When a user wants to update the records, the user can input the update in any format used by the user's local device. Whenever the patient information is updated, it will first be converted into the standardized format and then stored in the collection of medical records on one or more of the network-based storage devices. After the updated information about the patient's condition has been stored in the collection, the content server, which is connected to the network-based storage devices, immediately generates a message containing the updated information about the patient's condition. This message is transmitted in a standardized format over the computer network to all physicians and health-care providers that have access to the patient's information (*e.g.,* to a medical specialist to review the updated information about the patient's medical condition) so that all users can quickly be notified of any changes without having to manually look up or consolidate all of the providers' updates. This ensures that each of a group of health care providers is always given immediate notice and access to changes so they can readily adapt their own medical diagnostic and treatment strategy in accordance with other providers' actions. The message can be in the form of an email message, text message, or other type of message known in the art.

Claim 1:

A method comprising:

a) storing information in a standardized format about a patient's condition in a plurality of network-based non-transitory storage devices having a collection of medical records stored thereon;

b) providing remote access to users over a network so any one of the users can update the information about the patient's condition in the collection of medical records in real time through a graphical user interface, wherein the one of the users provides the updated information in a non-standardized format dependent on the hardware and software platform used by the one of the users;

c) converting, by a content server, the non-standardized updated information into the standardized format,

d) storing the standardized updated information about the patient's condition in the collection of medical records in the standardized format;

e) automatically generating a message containing the updated information about the patient's condition by the content server whenever updated information has been stored; and

f) transmitting the message to all of the users over the computer network in real time, so that each user has immediate access to up-to-date patient information.

Step	Analysis
Step 1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
Step 2A - Prong 1: Judicial Exception Recited?	**Yes.** The claim as a whole recites a method of organizing human activity. The claimed invention is a method that allows for users to access patients' medical records and receive updated patient information in real time from other users which is a method of managing interactions between people. Thus, the claim recites an abstract idea.
Step 2A—Prong 2: Integrated into a Practical Application?	**Yes.** The claim recites a combination of additional elements including storing information, providing remote access over a network, converting updated information that was input by a user in a non-standardized form to a standardized format, automatically generating a message whenever updated information is stored, and transmitting the message to all of the users. The claim as a whole integrates the method of organizing human activity into a practical application. Specifically, the additional elements recite a specific improvement over prior art systems by allowing remote users to share information in real time in a standardized

	format regardless of the format in which the information was input by the user. Thus, the claim is **eligible** because it is not directed to the recited judicial exception (abstract idea).
Step 2B: Inventive Concept?	**N/A.**

Claim 2:

A method comprising:

a) storing information about a patient's condition in a plurality of network-based non-transitory storage devices having a collection of medical records stored thereon;

b) providing access, by a content server, to users so that any one of the users can update the information about the patient's condition in the collection of medical records, and;

c) storing the updated information about the patient's condition in the collection of medical records in the plurality of network-based non-transitory storage devices.

Step	Analysis
Step 1: Statutory Category?	**Yes.** The claim recites a series of steps and, therefore, is a process.
Step 2A - Prong 1: Judicial Exception Recited?	**Yes.** The claim as a whole recites a method of organizing human interactions. The claimed invention is a method that allows for users to access and update patients' medical records and store the updated information which is a method of managing interactions between people. The mere nominal recitation of a generic content server and generic network-based storage devices does not take the claim out of the methods of organizing human interactions grouping. Thus, the claim recites an abstract idea.
Step 2A—Prong 2: Integrated into a Practical Application?	**No.** The claim as a whole merely describes how to generally "apply" the concept of storing and updating patient information in a computer environment. The claimed computer components are recited at a high level of generality and are merely invoked as tools to perform an existing medical records update process. Simply implementing the abstract idea on a generic computer is not a practical application of the abstract idea.
Step 2B: Inventive Concept?	**No.** As noted previously, the claim as a whole merely describes how to generally "apply" the concept of updating medical records in a computer environment. Thus, even when viewed as a whole, nothing in the claim adds

	significantly more (i.e., an inventive concept) to the abstract idea. The claim is **ineligible**.

Patents in the New Media

Moderator

Douglas A. Miro, Esq.
Partner
AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Panelists

Charles R. Macedo, Esq.
Partner
AMSTER ROTHSTEIN & EBENSTEIN LLP
Intellectual Property Law

Richard P. Zemsky,
Chief Operating Officer,
AIMeCAST

NYSBA Annual Meeting 2019
January 15, 2019
4:10 pm

DISCLAIMER

The following presentation reflects the personal opinions of its authors and does not necessarily represent the views of their respective employers, partners, clients or the NYSBA. Additionally, the following content is presented solely for the purposes of discussion and illustration, and does not comprise, nor is not to be considered, as legal advice.

–2

Agenda

Media Delivery

Patent Wars

Patent Challenges

Media Delivery

New Media Patent Wars

Patent Challenges

-3

Agenda

Media Delivery

Patent Wars

Patent Challenges

Media Delivery

+ Old Media Delivery
+ New Media Delivery
+ New Media Delivery Participants
+ New Media OTT Apps

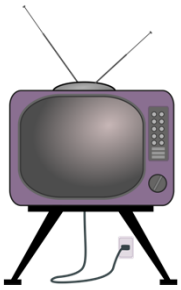
New Media Patent Wars

Patent Challenges

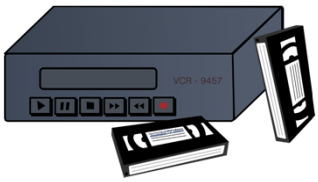
-4

Media Delivery

Old Media Delivery



TV



VCR

DVD

–5

Media Delivery

New Media Delivery

Internet website

Smart Phone, Computer and Tablets Apps

Apple TV (and other set top boxes) with TV

–6

Media Delivery

New Media Delivery Participants

Traditional Cable Companies

COMCAST, Charter COMMUNICATIONS, altice, COX, ETC.

Traditional Content Providers

CBS, abc, NBC, FOX, The CW, STARZ, HBO, SHOWTIME, ETC.

Telecos Offering Cable

DIRECTV, fios by verizon, ETC.

New SVOD Providers

NETFLIX, prime, hulu, sling TELEVISION, ETC.

"FANG"

facebook, YouTube, ETC.

–7

Media Delivery

New Media Delivery Participants

Content Management System Providers

COMCAST TECHNOLOGY SOLUTIONS, VUBIQUITY, ETC.

Encoders and Other Suppliers

encode.com, ETC.

Video Storage Farms

aws, rackspace, ETC.

Content Delivery Networks

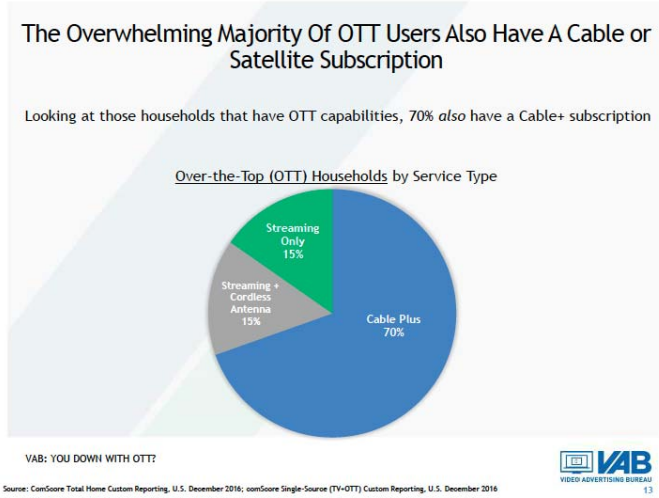
Limelight NETWORKS, Akamai, COMCAST, ETC.

Hardware/ Set Top Boxes

tv, Roku, amazon fireTV, ARRIS, SAMSUNG, ETC.

–8

Media Delivery

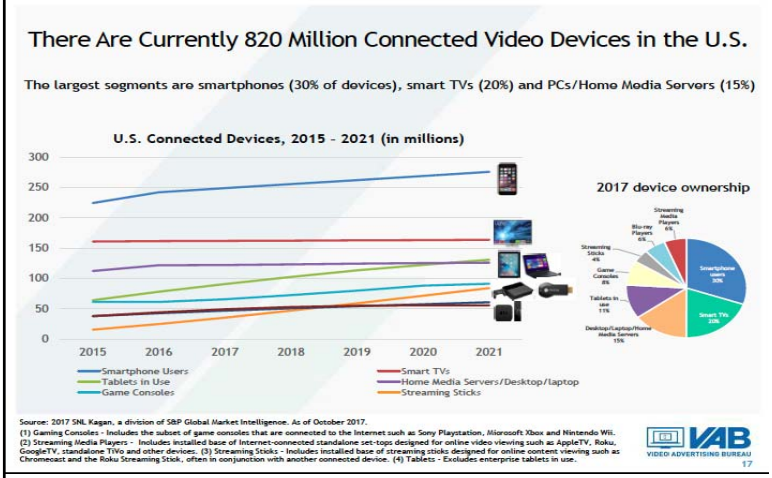


TAKEAWAY:
70% of Cable homes have OTT capabilities

http://www.thevab.com/wp-content/uploads/2018/03/OTT-Ecosystem-Overview-Final.pdf
(downloaded Dec. 31, 2018, p. 17)

–9

Media Delivery

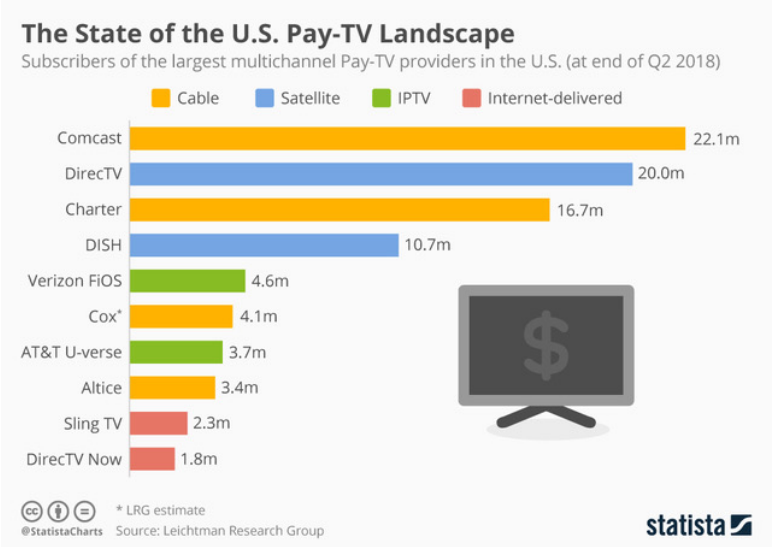


TAKEAWAY:
- 20% Smart TVs,
- 30% Smart Phone,
- 15% Desktop, Laptop, Home Media Servers,
- 11% Tablets
- 8% Game Consoles
- 4% Streaming Sticks
- 6% Streaming Media Players

http://www.thevab.com/wp-content/uploads/2018/03/OTT-Ecosystem-Overview-Final.pdf
(downloaded Dec. 31, 2018, p. 17)

–10

Media Delivery



–11

Agenda

Media Delivery

Patent Wars

Patent Challenges

Media Delivery

New Media Patent Wars

Patent Challenges

-12

New Media Patent Wars

Patent Owners: Realtime Adaptive Streaming LLC	
PTAB	7 IPRs (Netflix, Sony Corporation, Cisco Systems, Sling TV, Amazon.com, Hulu, Unified Patents, Inc.)
Cases in E.D. Tex.	5 (Cisco Systems, LG Electronics, Amazon.com, Samsung Electronics, Echostar Technologies)
Cases in C.D. Cal.	4 (Adobe Systems, Cox, Google, Hulu)
Cases in D. Colo.	8 (Comcast d/b/a Xfinity, Charter Advanced Micro Devices, Intel, Mitel, Avaya, Broadcom Wowza Media, Apple, Polycom, Sling TV)
Cases in D. Del.	4 (Netflix, Sony Electronics, Brightcove, Haivision)
Cases in D. Mass.	1 (Adobe Systems)

*All figures are estimates taken from Docket Navigator on January 7, 2019

–13

New Media Patent Wars

Patent Owners: Blue Spike, LLC	
PTAB	1 IPR (Kyocera)
Cases in E.D. Tex.	Over 140 cases (Altice, Charter, DISH, Comcast, Suddenlink, Roku, Rovi, Yahoo, Google, Shazam, etc.)
Cases in S.D.N.Y.	1 (Soundmouse)
Cases in D. N.J.	1 (Iris ID Systems)
Cases in D. Del.	5 (Charter, Comcast, SoundCloud, Roku)
Cases in D. Mass.	1 (Kronos)
Cases in C.D. Cal.	9 (SoundCloud, Deezer, Aspiro AB, Pandora Music, Spotify, Visual Land, Media Science, Vizio, 3M Cogent)
Cases in N.D. Cal.	8 (Toshiba, Facebook, Gracenote, Adobe Systems, Zeitera, SoundHound, Google, Juniper Networks)
Cases in S.D. Cal.	2 (ImageWare, Juniper Networks)

*All figures are estimates taken from Docket Navigator on January 7, 2019

–14

New Media Patent Wars

Patent Owners: Roku, Inc./TiVo, Inc.	
PTAB	3 IPRs (Samsung, Convergent Media Solutions, Hera)
ITC	4 (Macronix, Microsoft, STMicroelectronics, Rovi et al.)
Cases in C.D. Cal.	4 (Digital CBT, Sonicblue, Forgent Networks, Microsoft)
Cases in N.D. Cal.	2 (Echostar Communication, Digital CBT)
Cases in N.D. Ga.	1 (Echostar Communications)
Cases in N.D. Ill.	2 (Premier International Associates, Wild Cat Licensing)
Cases in D. Mass.	3 (Hybrid Auto, Lycos, Pause Technology)
Cases in S.D.N.Y.	2 (Asip, Digital Devel. Corp.)
Cases in E.D. Tex.	5 (Verizon, Samsung, Echostar, Cisco, AT&T)

*All figures are estimates taken from Docket Navigator on January 7, 2019

–15

New Media Patent Wars

Patent Owners: OpenTV, Inc.	
PTAB	5 IPRs (NFL Enterprises, Comcast, Apple, Netflix, Cisco Systems) and 1 CBM (Apple)
ITC	1 (ARRIS, Comcast, Gemstar, etc.)
Cases in E.D. Tex.	2 (NFL Enterprises, Verizon)
Cases in N.D. Cal.	3 (Apple, Netflix, Liberate Technologies)
Cases in D. Del.	1 (Netflix)
Cases in C.D. Cal.	1 (Hulu)

*All figures are estimates taken from Docket Navigator on January 7, 2019

–16

New Media Patent Wars

Patent Owners: Sprint Communications Company	
PTAB	2 IPRs (TC Technology, AIP Acquisition)
Cases in E.D. Va.	1 (Charter)
Cases in D. Del.	9 (WideOpenWest, TGP Global, Mediacom, IDT, Frontier Communications, Comcast, Charter, Crequel d/b/a Suddenlink, Atlantic Broadband Finance)
Cases in D. Kan.	9 (Vonage, TWC, Paetec, Nuvox, Cox, Cable One, Broadvox, Big River Telephone Company, Gammino)

*All figures are estimates taken from Docket Navigator on January 7, 2019

–17

New Media Patent Wars

Patent Owners: Broadband iTV, Inc.	
PTAB	1 CBM (Hawaiian Telecom) + 1 IPR (Unified Patents)
Cases in D. Haw.	2 (Time Warner Cable, Hawaiian Telecom)
Cases in N.D. Cal.	1 (OpenTV, Inc. - Contract dispute)

*All figures are estimates taken from Docket Navigator on January 7, 2019

–18

New Media Patent Wars

Sample of Serial Defendants	
Apple	100s of cases including IPRs (PTAB, ITC, E.D. Va., W.D. Tex., N.D. Tex., **E.D. Tex.**, D. Ut., W.D. Wa., N.D. Ill., D. Del., S.D. Cal., N.D. Cal., etc.)
Charter (also formerly Time Warner Cable)	About 20 cases plus 2 IPRs (PTAB, E.D. Va., E.D. Tex., D. Kan., **D. Del.**)
Altice (also Suddenlink/Cablevision)	Over 30 cases plus 1 IPR (PTAB, **D. Del.**, E.D. Tex., N.D. Ill., S.D.N.Y.)
Netflix	About 75 cases plus 10 IPRs and 1 CBM (PTAB, ITC, E.D. Tex., N.D. Tex., W.D. Tex., W.D. Wa., E.D. Va., **D. Del.**, N.D. Cal., D. Mass., C.D. Cal., ITC)
Hulu	About 40 cases plus 8 IPRs (PTAB, **E.D. Tex**., N.D. Tex., E.D. Va., N.D. Ill., D. Del., S.D. Cal., **C.D. Cal**., etc.)
Key jurisdictions for suits against serial defendants include **E.D. Tex.** and **D. Del.** Key issues involve patent invalidity and infringement.	

*All figures are estimates taken from Docket Navigator on January 7, 2019

–19

Agenda

Media Delivery

Patent Wars

Patent Challenges

Media Delivery

New Media Patent Wars

Patent Challenges

+Venue
+ Patent Eligibility
+ Divided Infringement
+ Indemnification

-20

Patent Challenges

Venue

Defendant State of Incorporation

OR

Where the defendant has committed acts of infringement and has a regular and established place of business

28 U.S.C. § 1400(b)

–21

Patent Challenges

Venue

Seven Networks, LLC v. Google LLC,
315 F. Supp. 3d 933, 960-61, 966 (E.D. Tex. 2018),
writ denied, 2018 U.S. App. LEXIS 31000 (Fed. Cir. Oct. 29, 2018)

"Here, the GGC [Google Global Cache] servers are best characterized as local data warehouses, storing information in local districts to provide Google's users with quick access to the cached data, avoiding the delays associated with distant data retrieval from Google Data Centers."

"The court concludes that the GGC servers and their locations within the various ISPs within this district are 'places of Google' sufficient to meet the statutory requirement of [U.S. Code Chapter 28 Section] 1400(b)."

–22

Patent Challenges

ITC — Domestic Industry

19 U.S.C. § 1337(a)(2)-(3)

(2) Subparagraphs (B), (C), (D), and (E) of paragraph (1) apply only if an industry in the United States, relating to the articles protected by the patent, copyright, trademark, mask work, or design concerned, exists or is in the process of being established.

(3) For purposes of paragraph (2), an industry in the United States shall be considered to exist if there is in the United States, with respect to the articles protected by the patent, copyright, trademark, mask work, or design concerned—

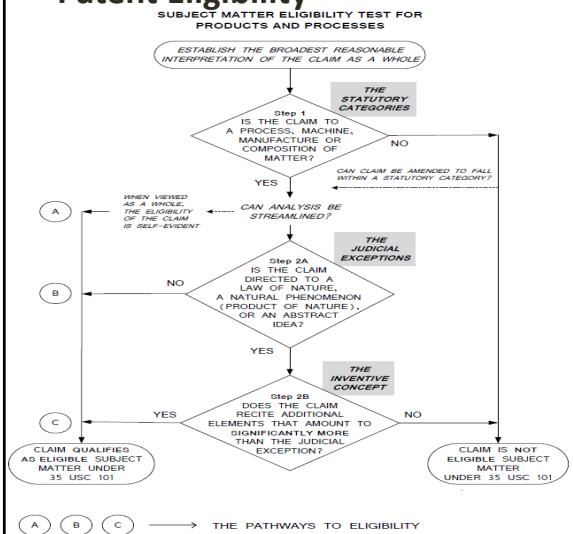
(A) significant investment in plant and equipment;
(B) significant employment of labor or capital; or
(C) substantial investment in its exploitation, including engineering, research and development, or licensing.

May be met by:

- Complainants own activities
- Licensee's activities

Patent Challenges

Patent Eligibility

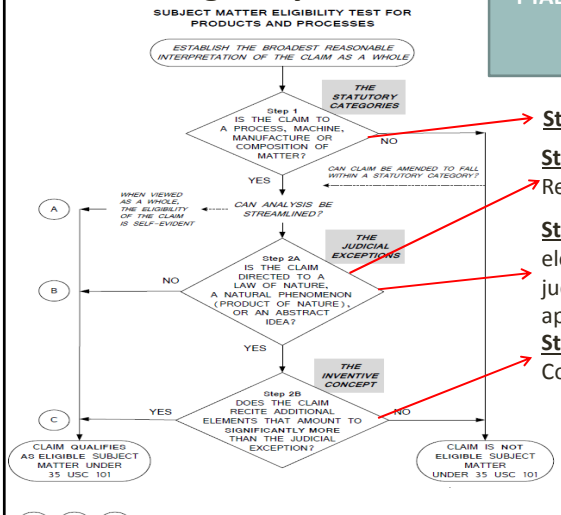


OLD STANDARD

From MPEP § 2106 - Patent Subject Matter Eligibility

Patent Challenges

Patent Eligibility



From MPEP § 2106 - Patent Subject Matter Eligibility

PTAB Guidance on Patent Subject Matter Eligibility (January 7, 2019)

Step 1: Statutory Category?

Step 2A Prong 1: Judicial Exception Recited?

Step 2A Prong 2: Are there additional elements that integrate the identified judicial exception into a practical application?

Step 2B: Claim provides an Inventive Concept?

–25

Patent Challenges

Step 1 & Step 2

Patent Eligibility

Trading Techs. Int'l v. CQG, Inc.,
675 Fed. Appx. 1001, 1004 (Fed. Cir. 2017) (unpublished)

- The patent claims cover a computerized method and system used for trading stocks and similar products.
- Under *Alice* step one, the Federal Circuit held that the patents solve problems of prior graphical user interface devices used for computerized trading. Specifically, the Federal Circuit stated that "the patents describe a trading system in which a graphical user interface 'display[s] the market depth of a commodity traded in a market" including various static and dynamic displays and this graphical user interface solves "'problems of prior graphical user interface devices…relating to speed, accuracy and usability.'" The Federal Circuit found that the patents presented patent-eligible subject matter.
- Under *Alice* step two, the court "determined that the challenged claims recite an 'inventive concept.'" The Federal Circuit agreed with the District Court's identification of the feature of "the static price index as an inventive concept" that permits more efficient and accurate trade placement when using electronic trading systems.

–26

Patent Challenges

Step 1

Patent Eligibility

Finjan, Inc. v. Blue Coat Sys.,
879 F.3d 1299 (Fed. Cir. 2018)

- Finjan filed a lawsuit against Blue Coat for infringement of four patents relating to computer software for identifying and protecting against malware. Claims were directed to behavior-based virus scanning, as opposed to the traditional code-matching method.
- The Federal Circuit affirmed the district court's finding that the claims were not directed toward an abstract idea for two reasons. First, the claims were drawn to behavior-based virus scanning which analyzes a downloadable's code and determines whether it performs potentially dangerous or unwanted operations. This was different than the traditional method of code-matching virus scanning. The Federal Circuit also determined that this was an improvement in computer functionality.
- Second, the results of the behavior-based virus scan are attached to a new type of file which enables a computer security system to perform tasks that it could not do before. Also, the claims recited more than a mere result and provided specific steps of generating a security profile that identifies suspicious code and links it to a downloadable.

–27

Patent Challenges

Step 1

Patent Eligibility

Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.,
880 F.3d 1356 (Fed. Cir. 2018)

- Core Wireless sued LG alleging infringement of patent claims directed to improved display interfaces, particularly for electronic devices with small screens. The improved interfaces allow a user to more quickly access data and applications in electronic devices.
- The Federal Circuit acknowledged that the generic idea of summarizing information existed prior to the invention. However, the Federal Circuit noted that the claims recite a specific improvement over conventional user interface methods, resulting in an improved user interface for electronic devices. In its analysis, the Federal Circuit pointed to claim limitations that disclose the specific manner of displaying a limited set of information to the user. It also highlighted language in the specification which indicates that the claims are directed to an improvement in the functioning of computers, particularly those with small screens. Because the Federal Circuit held that the asserted claims are not directed to an abstract idea, it did not proceed to the second step of the inquiry under *Alice*.

–28

Patent Challenges

Step 1 & Step 2

Patent Eligibility

Data Engine Techs. LLC v. Google LLC,
906 F. 3d 999, 1008-09 (Fed. Cir. 2018)

- The "Tab Patents" claims relate to techniques for making complex, 3-D spreadsheets more navigable via the use of familiar, user-friendly interface objects like notebook tabs.
- Applying *Alice* step one, the opinion describes how a representative claim was not directed to an abstract idea, but to "a specific method for navigating through three-dimensional electronic spreadsheets." It describes how the Tab Patents solved a known technological problem, in a particular way, and required a specific interface and implementation to do so. For the § 101 analysis, the opinion emphasizes the "functional improvement achieved by the specifically recited notebook tabs in the claimed methods."
- One Tab Patents claim was patent-ineligible however. Unlike the other claims, it did not recite the specific tab implementation of a notebook tab interface, and "cover[ed] any means for identifying electronic spreadsheet pages." This was directed to an abstract idea at *Alice* step one, and lacked any inventive concept at *Alice* step two.

–29

Patent Challenges

Patent Eligibility

PTAB Guidance on Patent Subject Matter Eligibility (January 7, 2019)

EXAMPLE 37

Claim 1:
A method of rearranging icons on a graphical user interface (GUI) of a computer system, the method comprising:
receiving, via the GUI, a user selection to organize each icon based on a specific criteria, wherein the specific criteria is an amount of use of each icon;
determining, by a processor, the amount of use of each icon over a predetermined period of time; and
automatically moving the most used icons to a position on the GUI closest to the start icon of the computer system based on the determined amount of use.

Step 1: Yes.
Step 2A - Prong 1: Yes.
Step 2A - Prong 2: Yes.
Step 2B: N/A

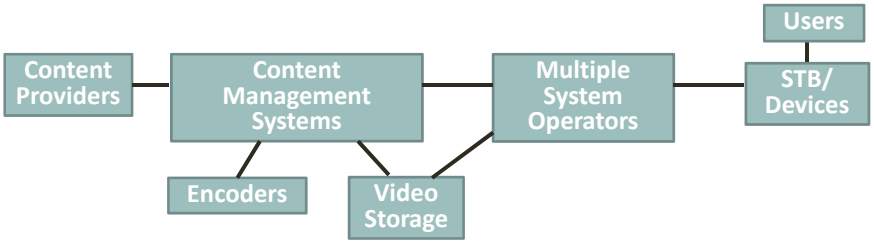
Claim 2:
A method of rearranging icons on a graphical user interface (GUI) of a computer system, the method comprising:
receiving, via the GUI, a user selection to organize each icon based on a specific criteria, wherein the specific criteria is an amount of use of each icon;
determining the amount of use of each icon using a processor **that tracks how much memory has been allocated to each application associated with each icon** over a predetermined period of time; and
automatically moving the most used icons to a position on the GUI closest to the start icon of the computer system based on the determined amount of use.

Step 1: Yes.
Step 2A - Prong 1: No.
Step 2A - Prong 2: N/A
Step 2B: N/A

–30

Patent Challenges

Divided Infringement



Because there are so many participants in a typical distribution of new media, it is important to understand who the infringer is.

Consider relationship of participants, passive claiming, necessary steps or equipment, etc.

–31

Patent Challenges

Divided Infringement

Akamai Techs., Inc. v. Limelight Networks, Inc., 797 F.3d 1020, 1022-23 (Fed. Cir. 2015)

"We will hold an entity responsible for others' performance of method steps in two sets of circumstances:

(1) where that entity directs or controls others' performance, and
(2) where the actors form a joint enterprise."

Liability can also be found "when an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance."

"**Direction or control**" can be found where "an alleged infringer conditions participation in an activity or receipt of a benefit upon performance of a step or steps of a patented method and establishes the manner or timing of that performance."

A controlling "mastermind" is still required to meet "direction or control" test, after *Akamai*.

A **joint enterprise** requires proof of four elements:

1) an agreement, express or implied, among members of the group;
2) a common purpose to be carried out by the group;
3) a community of pecuniary interest in that purpose, among the members; and
4) equal right to a voice in the direction of the enterprise, which gives an equal right of control.

–32

Patent Challenges

Divided Infringement

Eli Lilly & Co. v. Teva Paremteral Medicines, Inc., 845 F.3d 1357 (Fed. Cir. 2017)

- The Federal Circuit affirmed district court decision finding liability even though no single actor performed all steps.
- Under *Akamai*, the Court held physicians directly infringed the '209 patent by conditioning receipt of a benefit — receiving pemetrexed treatment — on patients' taking a specified dose of folic acid at a specified time (daily).
- The Federal Circuit rejected Defendants' argument that "mere guidance or instruction is insufficient to show 'conditioning' under *Akamai*," finding that conditioning "does not necessarily require double-checking another's performance or making threats."
- The Federal Circuit also rejected the defendants' argument that "an actor can only condition the performance of a step 'by imposing a legal obligation to do so, by interposing that step as an unavoidable technological prerequisite to participation,'" or both.

–33

Patent Challenges

Indemnification Statute

UCC § 2-312(3). Warranty of Title Against Infringement; Buyer's Obligation Against Infringement:

(3) Unless otherwise agreed a seller who is a merchant regularly dealing in goods of the kind warrants that the goods shall be delivered free of the rightful claim of any third person by way of infringement or the like but a buyer who furnishes specifications to the seller must hold the seller harmless against any such claim which arises out of compliance with the specifications.

–34

Patent Challenges

Indemnification Language & Negotiation

"Indemnitor hereby indemnifies Indemnitee against all and any damages that arise or result from claims of patent infringement brought by a third party subject to limitations as found in this agreement."

Details & Points of Negotiation:

Notice
Indemnitee must notify Indemnitor of the claim.

Right to Control Defense & Settlement
Indemnitor will likely require the right to control the litigation.
Does Indemnitee have input or veto power on settlement?

Limit on Amount
Cap amount of indemnification? Fixed cap? Cap at monies received from Indemnitee under the license?

Exclusions
No indemnity if claims arise from modifications to the products as delivered?

–35

Questions?

QUESTIONS

?

–36

Speaker Biographies

RICK BAKER, ESQ.

Biography

Rick Baker's law practice includes a mix of business transactions and litigation. The common thread of his work is providing advice and guidance to clients at those times most critical to them, whether in the midst of a dispute or when executing a strategic business move.

Rick has dedicated his legal career advocating for top Fortune companies, international businesses, and Georgia-based clients at the trial and appellate levels in Georgia and beyond. Outside of the courtroom, he represents private companies and individuals in a variety of industries in business formation, operation, and transfer. His extensive litigation experience enhances his ability to identify and mitigate areas of transactional risk.

What you can expect from Rick: A thoughtful and strategic approach, diligent and focused advocacy, and straightforward advice to achieve your goals.

Prior to forming Baker Jenner, Rick was a partner in a midtown Atlanta law firm. Before law school, he worked for a member of Congress and an incumbent gubernatorial candidate, coordinating grassroots campaign efforts and managing community affairs, media relations, and special events. He also has experience as a public relations counselor for corporate and non-profit entities.

Rick enjoys Atlanta's ATLA tennis league and getting away to the north Georgia Mountains.

BARRY M. BENJAMIN, ESQ.

Biography

BARRY M. BENJAMIN chairs Kilpatrick Townsend's Advertising and Marketing group, and is a partner in the firm's New York office. He focuses on advertising, intellectual property, technology, and privacy law. Mr. Benjamin regularly negotiates contracts for clients in various industries, including advertising industry contracts such as agency-client deals, co-promotion, talent, endorsement and sponsorship agreements, as well as technology and privacy oriented transactions such as licensing, data sharing, software development, and website development agreements. He also advises in the areas of consumer communication, advertising, and regulation, including all forms of marketing initiatives such sweepstakes, contests, social media engagement, direct mail, text, telemarketing, and charitable marketing programs.As an experienced litigator, Mr. Benjamin handles false advertising, trademark, trade dress, and copyright claims. Mr. Benjamin also has extensive experience representing advertisers and marketers in regulatory investigations before government agencies and in competitor challenges through the self-regulatory process (NAD, CARU). Mr. Benjamin is a frequent speaker and author on advertising, marketing, privacy, and emerging media issues, and has written articles in many different publications.

JEMAR E. DANIEL, ESQ.

Biography

Jemar E. Daniel is currently Vice President and Senior Counsel in Viacom Media Network's Business and Legal Affairs group. He provides production content review for various VMN client groups across digital and linear platforms. In his position, he advises clients on privacy, copyright, right of publicity, and legal issues presented in broadcast distributed on traditional, digital, and new media platforms.

Before joining VMN in 2014, Jemar was a member of BET's Business and Legal Affairs group. Jemar holds a Juris Doctor from American University, Washington College of Law and a Bachelor of Arts from McDaniel College. He is admitted to practice in New York.

CATHERINE M.C. FARRELLY, ESQ.

Biography

Catherine M.C. Farrelly is a partner and chair of the Trademark & Brand Management Group at Frankfurt Kurnit Klein + Selz PC. She is also a member of the firm's Litigation Group.

Ms. Farrelly is an internationally recognized leader in the field of trademark law, who advises some of the world's leading brands. She helps her clients build and protect their trademark rights throughout the world, through strategic portfolio development and combatting infringement. Her clients span a variety of industries, including entertainment, apparel, sports, e-sports, toys, finance, cosmetics, alcoholic beverages, and publishing.

A frequent presenter and author on IP topics, Ms. Farrelly chairs the ABA's USPTO Operations Relating to Trademarks Subcommittee and is the Vice Chair of its Trademark Litigation Committee. She is a member of the New York State Bar Association, the International Trademark Association, the Copyright Society, and the New York Intellectual Property Law Association. She also serves on the advisory board for the University of Pennsylvania Law School, Detkin Intellectual Property and Technology Legal Clinic.

ANTHONY FORD, ESQ.

Biography

Anthony supports Medidata's global data privacy and data governance programs; Anthony also focuses on data security and technology-driven issues in clinical trials and life sciences. Prior to joining Medidata, Anthony was an associate in the IP, Tech and Data Group at Reed Smith, where he focused on information governance, privacy, and data security issues impacting large organizations. Prior to becoming an attorney, Anthony was a computer scientist for six years with the U.S. Air Force Research Laboratory where he studied artificial intelligence and machine learning. His areas of specialty included genetic algorithms, computational epistemology, and dynamic human-machine teaming.

ANNE GORFINKEL, ESQ.

Biography

Anne Gorfinkel is the Vice President of Standards and Practices for the Nickelodeon Group at Viacom Media Networks. S & P interprets and applies guidelines to ensure that multi-platform content and advertising are safe and appropriate for intended audiences. Gorfinkel collaborates with creative teams and business units so that programming, production, promotion, marketing, advertising, digital media, consumer products, social media content and new lines of business meet regulatory, industry and self-regulatory standards, foremost among them the FCC's Children's Television Act, the FTC's COPPA rule, and guidelines put forward by CARU, the Children's Advertising Review Unit.

Gorfinkel's career is grounded in over 30 years of media production and broadcasting with principal roles in public media for non-fiction programming, news, and children's television. Prior to working at Nickelodeon, she owned ARG Media, a strategic consulting service for media companies, marketing agencies and non-profit organizations. Before creating her own agency, Gorfinkel helped to launch and then serve as Executive Director of *TheTakeaway*, a daily national news program for Public Radio produced by WNYC Radio and Public Radio International in partnership with the BBC World Service, The New York Times and WGBH Boston. Prior to joining WNYC, she launched educational children's programming for PBS under the auspices of WTTW/Chicago, the U.S. Department of Education, the Corporation for Public Broadcasting and the world-renowned Sesame Workshop, non-profit producer of *Sesame Street*. Gorfinkel served as VP of Project Development and Management for emerging properties at Sesame Workshop, and later as VP of Educational Outreach responsible for international *Sesame Street* co-productions in developing countries and community-based initiatives promoting literacy, healthcare and mutual respect and understanding.

Gorfinkel's formative experiences were at Thirteen/WNET, the flagship public television station where she was Deputy Director of Broadcasting for local and national programming, working with public television luminaries like Bill Moyers and Ken Burns, and production manager for the nightly news program, *MacNeil/Lehrer NewsHour.* She began her career at the innovative Television Laboratory at Thirteen/WNET working with independent filmmakers and documentarians on *Non Fiction Television*.

Gorfnkel graduated magna cum laude from Brown University with a BA in European History and still devours historical literature and drama. She lives in Montclair, NJ and has two adult sons, both of whom work in media despite her best efforts to see them earn a living.

JILL GREENWALD

Biography

Jill has been in-house counsel at ABC since June 2000. As Assistant Chief Counsel in the Legal Affairs Department, she focuses on negotiating and drafting contracts, as well as providing advice and counsel for many business units. Among her internal clients are ABC News, the ABC Television Network, ABC's owned and operated television stations, (with a focus on ABC's Stations in Philadelphia and Fresno), Good Morning America, The View, Promotions, Daytime, Broadcast Operations & Engineering, and the Research division. As part of The Walt Disney Company, some of her deals include working closely with her colleagues in other divisions of Disney, such as ESPN, and Disney Channel.

The substantive agreements she has worked on include: talent, production, research, special events (stunts and appearances), professional services, Software as a Service, product integration, promotions, distribution, publishing, music, software development, purchasing, satellite, venue, retransmission consent, and various content and licensing agreements.

In addition, she was appointed by the General Counsel in 2002 to act as Secretary for the Board of Directors of Lifetime Entertainment Services, a position which she held until 2010. In 2001, she was appointed to act as Secretary to the Board of Directors of A&E Television Networks for a one year term. She was appointed in 2008 as Counsel to Network News Service, a partnership between the News Divisions of ABC, Fox, and CBS, for a rotating one year term every three years.

In prior years, she as an active member on the Entertainment Law Committee (2001-2005) and the Copyright Committee (2006-2009) of the New York City Bar Association, as well as a member of the Intellectual Property Section, Trademark Committee, of the New York State Bar Association (1995-2000).

Before joining ABC, Jill was a litigator. She practiced commercial litigation for five years, and then specialized in intellectual property for five years, both on the litigation and the transactional side. Her last law firm stop was at Fried, Frank, Harris, Shriver & Jacobson, where she oversaw the worldwide trademark portfolio of Loews Cineplex Entertainment and handled trademark and copyright infringement actions, as well as performed due diligence for many high profile corporate transactions.

Jill graduated from Duke University, and received her law degree from Duke Law School. She lives in Manhattan with her young daughter and rescue dog Simba. In her free time, she enjoys theater, movies, museums, listening to live music and likes to play tennis, ski, travel and hit an occasional golf ball.

REBECCA GRIFFITH, ESQ.

Biography

Rebecca Griffith is a Senior Marketing Counsel for Unilever United States, where she has handled a variety of brands in the foods and refreshments categories. Prior to joining Unilever, Becky was a Senior Attorney and advertising review specialist for the National Advertising Division (NAD) of the Advertising Self-Regulatory Council (ASRC) where she resolved disputes over advertising claims in all forms of media and for a wide variety of industries, including Consumer Packaged Goods, Telecommunications, Dietary Supplements, and Insurance. Becky has also worked in private practice at leading law firms in New York where she specialized in branding and intellectual property protection. She earned her B.A. in English literature, cum laude, from the University of Pennsylvania, and her J.D. from New York University School of Law in 2002. In her spare time, Becky enjoys reading, travel, running and listening to podcasts.

NUR-UL HAQ, ESQ.

Biography

Nur-ul-Haq is Vice President, Counsel, Kids' Compliance at Viacom, where he advises on legal and regulatory compliance with the various laws and regulations relating to children, including the Federal Trade Commission Act (FTC Act), the Children's Online Privacy Protection Act (COPPA), the Children's Television Act (CTA), the Child Protection and Obscenity Enforcement Act of 1988, among others.

Prior to joining Viacom, Nur was Privacy Counsel, Americas for NBCUniversal, focusing on privacy and information security matters in the US, Canada, and Latin America relating to all divisions of the business, including film, news, entertainment, cable, digital, theme parks, movie ticketing, and internal business operations. Previously, Nur served as a staff attorney in the Federal Trade Commission's Northeast Regional Office, where he led and participated in investigations and litigations relating to deceptive marketing and advertising practices, anticompetitive practices, and violations of various FTC rules. In that role, Nur also performed extensive consumer and business outreach on privacy, information security, identity theft, consumer credit, and other topics.

Nur is a graduate of Georgetown University and Boston University School of Law, cum laude, and is a member of the American Bar Association sections of Antitrust Law and Science and Technology Law, the New York State Bar Association, the Massachusetts Bar Association, and the International Association of Privacy Professionals.

LEONIE HUANG, ESQ.

Biography

Leonie Huang is a litigation attorney in Holland & Knight's New York office and a member of the firm's Intellectual Property Group. Ms. Huang practices in the areas of intellectual property and technology-driven litigation as well as complex commercial litigation and business tort defense.

Ms. Huang has represented clients in patent litigation, including Hatch-Waxman patent litigation, trademark, copyright, contract and licensing disputes, breach of contract and related business tort litigation, shareholder disputes and in the defense of product liability in toxic tort claims. Ms. Huang assists clients in a wide range of technologies and product areas, ranging from pharmaceuticals and biotechnology to consumer technology and goods. Ms. Huang focuses her pro bono work in the area of criminal defense.

Prior to attending law school, Ms. Huang worked at the Administrative Office of the U.S. Courts as a budget analyst for the federal courts. She served as an analyst and support staff to the Judicial Conference Budget Committee in the areas of Defender Services and Probation and Pretrial Services.

While attending law school, Ms. Huang was a notes & articles editor of the *Fordham Law Review* and a member of the Fordham Moot Court Board. Ms. Huang was awarded the Archibald R. Murray Public Service Award for her work at the Fordham Law Criminal Defense Clinic. She also received the "Class of 1911" Award for the best essay submitted by a student in the graduating class on a legal subject designated by the Dean.

Honors & Awards

- New York State Bar Association, Intellectual Property Law Section Fellow, 2016-2017

Education

- Fordham University School of Law, J.D.
- American University, MPA
- Georgetown University, B.S., Honors Certificate in International Business Diplomacy

Bar and Court Admissions

- New Jersey (State courts and U.S. District Court for the District of New Jersey)
- New York (State courts and U.S. District Courts for the Eastern and Southern Districts of New York)
- U.S. Court of Appeals for the Federal Circuit and U.S. Court of Appeals for the Second Circuit

RICHARD S. EISERT, ESQ.

Biography

Richard S. Eisert is co-chair of the Advertising, Marketing & Promotions Practice Group and a partner in the Intellectual Property and Digital Media, Technology & Privacy Practice Groups of Davis & Gilbert. His clients include new media, technology and telecommunications companies, traditional publishing entities, advertisers, and advertising agencies.

His traditional advertising/marketing law practice includes the review of advertising copy, advising with regard to issues such as claim substantiation, false advertising and related intellectual property and privacy/publicity issues, and negotiating and drafting a broad array of contracts, including agency/client agreements, media buying agreements, sponsorship agreements and strategic alliances. In the new media area, his practice includes drafting and advising on contracts related to worldwide web sites, on-line advertising and commerce, and multimedia, software, music and technology licensing. Mr. Eisert's practice also includes advising on specific legal/regulatory issues that affect e-commerce, including privacy and the enforceability of electronic transactions. In the intellectual property arena, he advises on the protection, maintenance, and licensing of copyrights, trademarks, patents and trade secrets.

Mr. Eisert also represents clients in advertising arbitration proceedings before the NAD and advises clients with respect to litigations and regulatory proceedings that arise in the advertising/intellectual property arena. He also performs transactional due diligence and transfers of intellectual property in conjunction with corporate transactions such as mergers, acquisitions, financings, and securities offerings. He has considerable experience negotiating complex technology ventures in high technology and telecommunications, including representing international wireless carriers in connection with their wireless data, entertainment, digital music distribution, and information services.

Mr. Eisert has been involved in several initiatives to standardize legal terms for conducting business on the Internet. He served as a Law Clerk to the Hon. William C. Conner, in the Federal District Court for the Southern District of New York. While in law school, Mr. Eisert served as the Editor-In-Chief of the Harvard Journal of Law and Technology.

Mr. Eisert has been recognized by The Legal 500 United States in the area of advertising and marketing (2009-2018) and cyber law: data privacy and protection (2012-2018). He has also been recognized by The Best Lawyers in America in advertising law (2019) and ranked as a leading advertising lawyer by Chambers USA: America's Leading Lawyers for Business (2009-2016).

JESSICA B. LEE, ESQ.

Biography

Jessica works at the intersection of data, emerging media technology and leads Loeb & Loeb's Privacy, Security & Data Innovations Practice. Jessica counsels U.S., E.U. and multi-national clients on the privacy and intellectual property issues that arise when launching, marketing and monetizing digital products and content. With a deep understanding of her clients' business and the technologies they are looking to leverage, she is able to give business-focused, practical advice to clients looking to navigate the legal landscape of global privacy laws. Jessica advises on U.S. and European data protection laws and works with clients to develop comprehensive data protection strategies. On a daily basis, Jessica analyzes the issues associated with her client's advanced advertising strategies and helps clients leverage consumer insights in a privacy-compliant manner. She also has extensive knowledge of intellectual property and social media law and regularly counsels clients on everything from engaging influencers to using user generated content to optimize data collected through social media campaigns. Jessica has experience reviewing and drafting a variety of agreements, including content licensing agreements, agency-service agreements, sponsorship agreements, website policies, licensing agreements and releases. Jessica is a frequent speaker on issues involving privacy and technology, and has contributed to MarTech Today, AdAge, AdWeek and the Marketplace Tech podcasts, among other programs. Jessica is also the Co-Chair of Loeb's Affinity Group for Attorneys of Color and Ethnic Diversity ("ACED").

Jessica B. Lee, CIPP/US, CIPP/E, CIPM

Partner, Co-Chair, Privacy, Security & Data Innovations

MARC LIEBERSTEIN, ESQ.

Biography

Marc is the co-chair of the Retail & Consumer Goods industry team. His practice focuses on intellectual property licensing and franchising in the retail/consumer goods and services areas, fashion/apparel and accessories, food and beverage, and commercial/industrial design, including the drafting, negotiation and enforcement of license and franchise documents and agreements, as well as implementation of branding and commercialization objectives for clients via licensing and franchising. In conjunction with the services above, he counsels clients on creating effective strategies for procuring, protecting and enforcing their global intellectual property assets. Marc has also participated in and used alternative dispute resolution forums such as arbitration and mediation to enforce intellectual property rights. Marc frequently lectures and writes on intellectual property issues for a variety of intellectual property organizations and publications, including International Trademark Association (INTA), New York State Bar Association (NYSBA) Intellectual Property Section, American Bar Association Forum on Franchising, Wharton Business Law Association at the University of Pennsylvania, New York University, Association of the Bar of the City of New York Fashion Law Committee, Licensing Industry Merchandisers' Association (LIMA), *National Law Journal, IP Strategist* and *The New York Law Journal, Practical Law, The Licensing Journal*.

Marc is listed in the 2018 and the seven years immediately preceding editions of *World Trademark Review 1000 – The World's Leading Trademark Professionals*. He was recognized as a New York "Super Lawyer" in Intellectual Property by *Super Lawyers* magazine in 2018 and the eight years immediately preceding, and, for the last seven years, he was named a Top 100 New York Metro "Super Lawyer" in Intellectual Property. Marc has been recognized as an "IP Star" in 2018 and the five years immediately preceding by *Managing Intellectual Property* magazine. In 2017, he was recognized by *Who's Who Legal* for Franchising. Marc was named a 2018 Legal Eagle by *Franchise Times.* He was also recommended by *Legal 500 US* in 2015, 2016, 2017 and 2018 for Copyright. In 2013, Marc received the Lexology *Client Choice Guide - International 2013* Award and is the sole winner in the Intellectual Property: Copyright category for New York. He was also listed in the 2012 and the four years immediately preceding editions of *Chambers USA: America's Leading Lawyers for Business* for Intellectual Property: Trademark & Copyright. Chambers noted that Marc has "tremendous business savvy and is tenacious in his work ethic," according to his clients (2012).

The International Trademark Association (INTA) honored Marc with the Volunteer Service Award (VSA) in the Advancement of Committee or Subcommittee Objectives category. The VSAs recognized Marc in 2015 for providing exemplary volunteer service to INTA. As a member of INTA's Alternative Dispute Resolution Committee's Neutral Standards & Measurement Subcommittee, Marc made a tremendous impact by volunteering both his time and expertise to support the Association's goals and objectives. Marc is a recipient of the 2015 Commitment to Justice Award presented by Her Justice recognizing his pro bono work in representing a client who sought help in terminating her arranged marriage. Through skillful negotiation, without any court intervention, Marc secured for the client a divorce on terms very favorable to her and to her children. He is a recipient of the Kilpatrick Townsend 2014 Pro Bono Justice Award. Marc is also a recipient of the 2015 Cardozo Law School Alumni of the Year Award recognizing Marc's leadership and dedication to Cardozo Alums and students.

ANTHONY LOCICERO, ESQ.

Biography

An engineer by training, Anthony Lo Cicero has represented companies in patent and trademark litigation involving product areas as diverse as e-commerce platforms, angular rate sensors, camcorders and flat panel displays. He conducts due diligence of IP portfolios and provides strategic patent counseling to companies in a wide range of industries from recorded and published music to consumer electronics. Most recently, he was the President of the New York Intellectual Property Association.

Very sophisticated technology competes with style and price as key aspects of the customer experience in the fashion industry. Mr. Lo Cicero represents some of the most prominent brick-and-mortar and on-line retailers in the country in patent disputes relating to the enterprise's e-commerce, mobile and point of sale systems. The retail industry regularly confronts patent assertions involving mobile platforms, electronic merchandise presentation, billing, marketing, inventory management and other features of the 21st century marketplace. Mr. Lo Cicero evaluates and responds to these assertions in a practical, business-oriented manner. Mr. Lo Cicero also evaluates contractual terms with vendors and suppliers to mitigate liability and works with retailers to identify and obtain protection for their own innovations. He has assisted retailers in successfully pursuing indemnification claims ranging to seven-figure settlements.

Restaurants, financial institutions, insurance companies, health care institutions, consumer product manufacturers and other businesses likewise rely on technology to bind customers, improve the customer experience, differentiate themselves and stimulate demand. Mr. Lo Cicero advises clients on freedom to operate issues, prosecutes patents and defends them in litigation.

Many of the most prestigious apparel manufacturers and retailers in the world, along with financial services, food products, computer, consumer electronics, home products, and toy companies also turn to Mr. Lo Cicero for trademark protection. He advances brand development and enforcement strategies ranging from anti-counterfeiting and trademark infringement protection to trade dress and Internet domain matters. For example, he overcame significant legal obstacles to protecting a name and symbol for what is now one of the best-known prestige brands in the country. On many occasions, he has been called upon to enforce trademark rights for entities that that do not have the advantage of a federal trademark registration.

In the public sector, Mr. Lo Cicero has been active in advocating responsible patent reform and he was actively involved in shaping the Trademark Anti-counterfeiting Act of 1984, and served on the board of the International Anti-counterfeiting Coalition during seminal efforts to strengthen the protection of federal and state laws, including Customs laws, to counteract counterfeiting. He is also effective at marshalling law enforcement agencies in the United States and other countries to disrupt and dismantle counterfeiting operations harming his clients' rights. For example, counterfeit toner cartridges were adversely

impacting the profitability of a major printer manufacturer; he coordinated Customs and law enforcement in the United States and abroad, obtained seizure orders and mitigated the problem. Similarly, he represents companies based in Europe, Asia and Latin America in protecting their trademark rights in the United States.

An important element of Mr. Lo Cicero's work is transactional and results in monetizing a client's IP through a sale or license agreement. Knowledgeable of customs and terms in a wide variety of industries, he counsels clients on structuring and pricing transactions when the IP is the key value of an enterprise.

Mr. Lo Cicero is immediate past President of the New York Intellectual Property Law Association. He also serves on the Board of Directors of Education for Music, a not-for-profit institution bringing music education and its attendant benefits to inner city children. He is a frequent speaker on issues of patent infringement, trademark dilution, anti-counterfeiting, arbitration, intellectual property damages and recovery, domain name disputes and Internet-related issues. He has been named a "Super Lawyer" for Intellectual Property and is included in IP Stars.

CHARLES R. MACEDO, ESQ.

Biography

Charles R. Macedo, a physicist by training, litigates in all areas of intellectual property law, including patent, trademark and copyright law, with a special emphasis in complex litigation and appellate work. Companies and individuals from a wide range of industries turn to him to develop offensive and defensive strategies for the development and enforcement of their patent and trademark portfolios.

Fluent in technical jargon spoken by inventors and clients, patentese spoken at the PTO, legalese spoken by courts and attorneys, business jargon spoken by management, and plain English, he seeks to translate complex subject matter into terms all can understand.

The author of The Corporate Insider's Guide to U.S. Patent Practice, Mr. Macedo has been cited as an authority on intellectual property issues by the Wall Street Journal, Dow Jones, BNA, Bloomberg, Inside Counsel, Managing Intellectual Property, Technology Transfer Tactics, IP Law 360, JIPLP and other media.

His patent experience encompasses a broad range of industries and products including Internet, e-commerce, content delivery and computer-enabled inventions; financial services, transaction processing, electronic wallets and virtual or synthetic currency, including Bitcoins and all other Alt-coins; Software-As-A-Service; social media; semiconductor and photomasks; green energy and power, including wind generators and batteries; construction materials and structures; life sciences; and apparel, to name a few. Mr. Macedo also has enforced and defended against trademark assertions and/or opposition proceedings for financial service providers, casinos and resorts, non-profit organizations, celebrities; cosmetic companies, luxury retailers of designer handbags and retail chains. He also advises clients on IP contracts, licensing, confidentiality agreements, terms of services and IP acquisitions and transfers.

By identifying vulnerabilities and considering variations on design concepts, Mr. Macedo helps clients develop strategies to maximize protection and prevent infringement challenges. He frequently serves as special counsel to companies seeking an IP strategy, not just a patent; to IP holders in anticipation of litigation and as coordinating counsel for multiple law firms.

He is consistently at the forefront of complex and emerging patent issues in the financial services and transaction processing industries. Clients ranging from international banks, broker dealers and new business ventures call on Mr. Macedo to develop patent strategies, prepare patents, assert rights and defend against infringement claims. His work includes developing and implementing patent strategies associated with such cutting edge financial innovations like bitcoins and other synthetic currency or math-based assets. His experience includes successfully defending the Discover Card division of Morgan Stanley from one of the earliest business method patent assertions, and leading the team to implement and enforce the deposit sweep patent portfolio for Island Intellectual Property LLC. He has also

helped clients implementing insurance related products seek patent and other intellectual property protection.

His experience before the Patent Trial and Appeals Board and its predecessor Board of Patent Appeals and Interferences, including acting as leading counsel in inter partes review and covered business method proceedings, as well as advising and analyzing in the background. He also has represented patent owners in ex parte appeals, including reversals of obviousness rejections in Ex parte Buarque de Macedo.

Mr. Macedo writes prolifically and lectures regularly as he tracks and analyzes in real time the most important developments affecting IP strategy and litigation. As Co-Chair of the Amicus Committee of the New York Intellectual Property Law Association, Mr. Macedo has been principal counsel or additional counsel on amicus briefs in some of the leading patent cases of recent years, including Cuozzo (at Federal Circuit en banc petition, Supreme Court petition for certiorari and merits brief stage), Highmark and Octane (at the Supreme Court), Kimble v. Marvel (at the Supreme Court), Mayo v. Prometheus (at the Supreme Court), Association of Molecular Pathology v. Myriad Genetics Inc. (at the Supreme Court and the Federal Circuit), CLS Bank Int'l v. Alice (at the Federal Circuit en banc and at the Supreme Court in the petition and merits brief stage), and Akamai (at the Federal Circuit on remand). His appellate experience also includes petitions for mandamus, for rehearing before the U.S. Court of Appeals for the Federal Circuit and for certiorari to the U.S. Supreme Court on behalf of various clients.

He holds bachelors and masters degrees in physics from The Catholic University of America and a law degree from Columbia Law School, all with honors. He was the sole law clerk to Hon. Daniel M. Friedman of the U.S. Court of Appeals for the Federal Circuit, 1989–1990. The recipient of the prestigious AIPLA Robert C. Watson Award, Mr. Macedo is included in Super Lawyers, IP Stars and Million Dollar Verdict. He also was a member of the Editorial Board for the American Intellectual Property Law Association Quarterly Journal and currently serves on the Editorial Board for Journal of Intellectual Property Law and Practice published by Oxford University Press.

DANIELLE E. MAGGIACOMO, ESQ.

Biography

Danielle Maggiacomo is an associate of the Trademark & Brand Management Group at Frankfurt Kurnit Klein + Selz PC.

Ms. Maggiacomo assists emerging and established companies with the creation, growth, and maintenance of global trademark portfolios, including clearance and application filing strategies. Ms. Maggiacomo also develops and implements enforcement initiatives including Uniform Domain Name Dispute Resolution Policy proceedings cease and desist letters, Internet takedowns, and litigation before the federal courts and the Trademark Trial and Appeal Board.

Ms. Maggiacomo serves as an Executive Committee member of the New York State Bar Association's Intellectual Property Section, a Leadership Board member of the Lehigh Lawyers Association, an Executive Committee Member of the Benjamin N. Cardozo School of Law Alumni Association, and as a member of INTA's Unreal Campaign committee.

MARK S. MELODIA, ESQ.

Biography

Mark Melodia is a privacy, data security and consumer class action defense lawyer in Holland & Knight's New York office. Mr. Melodia focuses his practice on governmental and internal investigations, putative class actions and other "bet-the-company" suits in the following areas: data security/privacy, mortgage/financial services and other complex business litigation, including defamation.

Mr. Melodia has defended more than 80 putative class actions – including as lead defense counsel in multiple multidistrict litigations (MDLs) – arising from alleged consumer privacy violations, data incidents and allegations of data misuse. Mr. Melodia is currently defending a global manufacturer of smart household devices against a putative class action arising from the alleged improper and undisclosed collection, storage, use and sale of private consumer information. He routinely represents clients responding to government privacy investigations before the Federal Trade Commission (FTC), Office for Civil Rights, state attorneys general and the U.S. Department of Justice (DOJ). He has guided clients in a wide range of industries through several hundred data incidents over the past dozen years. He advises clients on their obligations and helps them operationalize the requirements of General Data Protection Regulation (GDPR) as well as federal and state laws in the U.S. He consults with boards and executive teams on these issues.

Mr. Melodia has been an instructor of Information Security Law in the Chief Information Security Officer (CISO) Executive Education and Certification Program at Carnegie Mellon University's Heinz College, as well as a guest lecturer at Seton Hall Law School and New York University School of Law.

Mr. Melodia served as a law clerk for the Honorable Timothy K. Lewis of the U.S. District Court for the Western District of Pennsylvania.

Honors & Awards

- *National Law Journal*, Cybersecurity & Data Privacy Trailblazer, 2015
- *Law 360,* MVP in Privacy & Consumer Protection, 2011
- New Jersey *Super Lawyers* magazine, Class Action and Mass Torts, 2005-2006, 2014-2015, 2017-2018
- *NJ Biz*, 40-Under-40, New Jersey's Most Successful Business People, 2003
- The Order of Barristers, National Member
- New York University School of Law Moot Court Board, Competitions Director; Executive Committee

Education

- New York University School of Law, J.D., cum laude
- Princeton University, Woodrow Wilson School of Public and International Affairs, A.B., cum laude

Bar Admissions

- New York
- New Jersey
- Pennsylvania

DOUGLAS A. MIRO, ESQ.

Biography

Douglas A. Miro litigates patent, trademark, unfair competition and trade secret cases in district and appellate courts throughout the country. Mr. Miro is involved in patent litigation and patent prosecution in a wide variety of arts, including mechanical, electrical, ceramics, steel making, refractories, medical devices, and Internet related technologies. He counsels businesses and hospitals on a broad range of intellectual property issues, including establishing intellectual property programs, and on licensing and technology transfer matters. Mr. Miro also works in other intellectual property fields including copyrights, deceptive trade practices, and in all phases of intellectual property litigation.

MANAS MOHAPATRA, ESQ.

Biography

Manas Mohapatra is Senior Vice President and Chief Privacy Officer at Viacom, where he leads the Company's privacy and data protection efforts across the globe. Prior to joining Viacom, Manas held a number of positions at Twitter, including Head of Privacy and Data Protection and Associate General Counsel, Products. Before Twitter, Manas was a consumer protection attorney at the Federal Trade Commission, where he enforced federal privacy and consumer protection laws. At the FTC, Manas brought enforcement actions in multiple cases involving allegations of unfair or deceptive privacy and security practices, including the FTC's settlements with Facebook and MySpace. He co-authored the *FTC Staff Report: Mobile Apps for Kids: Disclosures Still Not Making the Grade* and also served on detail as an attorney-advisor to then-FTC Commissioner Edith Ramirez. Prior to joining the FTC, he was a litigation associate at Goodwin Procter, and a judicial law clerk for the Chief Judge of the U.S. District Court in Puerto Rico. Before law school, Manas worked as a senior web developer for Nickelodeon Online and as a database programmer for a distance education software company. He received his bachelors' degree from Johns Hopkins University and his law degree from Northwestern.

THEODORE C. NITTIS, J.D.

Biography

Theo is a nationally-known risk management and claims advocacy resource, as well as a former professional liability and insurance coverage litigator. He works closely with Gemini's larger law firm clients and is responsible for claims handling, and risk management consulting.

Theo received his undergraduate degree from Albion College, and his J.D. from Wayne State University. After leaving the private practice of law in 2003, he worked for national and regional insurance brokerages as a professional liability broker, claims advocate, and risk management resource.

In addition to presenting to numerous law firms around the country, Theo has lectured or been on discussion panels at dozens of legal malpractice and ethics conferences. He maintains active membership in the State Bar of Michigan, the Association of Professional Responsibility Lawyers, and the Council on Litigation Management.

When he isn't dissecting claims trends and law firm profitability, Theo spends his time with his wife, two children and bird dog. Only one of these family members greets him at the door when he comes home from the office; he'll let you figure out which one!

JOHN REED, ESQ.

Biography

Having worked with lawyers and law firms for more than 20 years, John Reed knows firsthand the challenges confronting the profession and the changing legal landscape. With a unique background in marketing and law, he collaborates with his clients to forge new strategies and stay ahead of the curve.

John began his marketing career with the lead advertising agency for a U.S. auto manufacturer, where he worked with national and international accounts in pursuit of the company's worldwide goals before changing gears and pursuing a law degree. After law school, he joined a large Midwest firm, gaining insight into the business of law and the unique issues lawyers and legal marketers encounter each day.

John left the practice for a successful career in the legal information industry, consulting with law firms of all sizes to provide solutions to their business development, competitive intelligence, professional development, and practice workflow needs. He was then recruited by a preeminent law firm public relations company to oversee its marketing and creative groups and lead its business development efforts.

Rain BDM is the culmination of John's special talents, and a natural outlet for his expertise. He trains and coaches attorneys to help them cultivate stronger client relationships, build bigger books of business, and gain new perspectives about the value of their services, and partners with law firms to enhance brand awareness, craft and promote their unique value propositions, and generate business development and marketing mindsets.

DEBORAH A. ROBINSON, ESQ.

Biography

Deborah Robinson is Vice President & Senior Counsel, Anti-Piracy, in Viacom's Law Department. She is responsible for the development and implementation of anti-piracy protocols, creation of enforcement strategies, and oversight of content protection operational workflows. She is also responsible for facilitating anti-piracy employee awareness programs and creating and conducting employee training programs.

Prior to joining Viacom, Ms. Robinson was Regional Counsel in the Anti-Piracy Legal Affairs Department for the northeast, central and southern regions of the Recording Industry Association of America (RIAA). She was responsible for monitoring and assisting with state and federal criminal investigations and prosecutions for the illegal duplication and distribution of sound recordings in 39 states, the District of Columbia and Puerto Rico. She also provided music piracy litigation training to prosecutors.

Ms. Robinson completed seven years of service as an assistant district attorney in Philadelphia, Pennsylvania. As a prosecutor, she was responsible for the successful prosecution of hundreds of major felony trials, including several high profile cases. During her last two years of service, she was the assistant chief of the Municipal Court Unit, where she was responsible for supervising 35 attorneys and the litigation of 65,000 cases each year.

Before becoming a prosecutor, Ms. Robinson was an associate at the law firm of Crawford and Associates in Philadelphia, practicing personal injury, entertainment and corporate law. She also served as legal counsel to the International Association of African American Music.

Ms. Robinson has shared her expertise as a television legal analyst on several networks, including ESPN, CNN Headline News, and Comcast CN8. She has also written articles for ESPN.com.

She received her J.D. degree from the University of Pittsburgh School of Law and holds a B.A. degree in economics from Howard University.

DAVID STONEHILL, ESQ.

Biography

David is Senior Vice President, Business & Legal Affairs and Deputy General Counsel of Viacom Media Networks. In this capacity, David oversees the centralized business and legal affairs team supporting multiplatform ad sales and operations, app development, platform distribution, business development, digital, advanced advertising, insights, audience science and measurement, program enterprises, information technology services, and rights management across Viacom Media Network as well as managing the business and legal affairs function for AwesomenessTV, a multiplatform media company and TV and film studio operated by Viacom Digital Studios. Prior to joining Viacom in 2007, David worked at several startups, including theglobe.com, where he was general counsel, and at the law firm of Richards & O'Neil. Before attending law school, he worked in the film business, both in development, as the Story Editor at Double Play Productions, and in production. David graduated from the University of Virginia School of Law in 1996 and magna cum laude from Brown University in 1991, with a BA in Classics. He lives in New York with his wife and two sons.

ADRIAN DEREK STUBBS, ESQ.

Biography

Adrian Stubbs joined CBS in April 2013 and now serves as Assistant General Counsel, CBS Television, where he supports the Sports Division with a variety of matters, including structuring, negotiating, and drafting agreements for CBS Sports Inc.'s and CBS Sports Network's multiple business units.

Adrian's areas of expertise include talent agreements and programming agreements, as well as advising clients on various intellectual property and marketing related matters.

Prior to joining CBS, Adrian was an attorney for WNET, where he counseled the production units responsible for Nature, Secrets of the Dead, and American Masters. He has also previously worked in the business & legal affairs department at CBS Interactive Inc.'s College Sports Division and as a full-time legal intern for CBS Sports Network when it was branded as CBS College Sports Network.

Adrian earned his J.D. from New York Law School and is admitted to the State Bar of New York. He attended Iona College in New Rochelle, New York and earned a Bachelor of Arts in Mass Communications, specializing in television production.

MATTHEW C. WINTERROTH, ESQ.

Biography

As Vice President of Intellectual Property, Matthew C. Winterroth leads enforcement of World Wrestling Entertainment Inc.'s ("WWE's") extensive intellectual property portfolio by way of implementation and administration of an integrated and aggressive anti-counterfeiting program and online anti-piracy program.

At WWE, Mr. Winterroth counsels internal business groups regarding the best branding strategy for developing, enhancing and protecting strong intellectual property rights worldwide, and aggregates/harmonizes collected data to assist in overall corporate strategy.

As a result of his years in private practice, as well as his current employment with WWE, Mr. Winterroth has represented various IP ownership rights in numerous industries, including live and televised sports entertainment, digital media, apparel, toys and sporting goods, national defense, hospitality and gaming, medical devices, home video, and theatrical films.

Mr. Winterroth received his Bachelor of Arts degree in Computer Science from Hamilton College in 1999, and his Juris Doctor from the University of New Hampshire (fka Franklin Pierce Law Center) in 2006. He is admitted to practice in New York, New Jersey, Connecticut and Pennsylvania.

RICHARD P. ZEMSKY, ESQ.

Biography

Richard P. Zemsky, an attorney and entrepreneur, is co-founder and Chief Operations Officer of Neurovation Labs. Mr. Zemsky received a B.S. in Mechanical Engineering from Villanova University before graduating from Columbia Law School. He founded Sproute Travel, a tech company for travel recommendations and trip planning. Richard has previously conducted research in heat transfer theory, shape memory alloy-based robotic design, and sediment accumulation on mid-ocean ridges, and served as team lead for mechanical and aeronautical design for a vertical take-off and landing electric aircraft.

As an attorney he focused on patent law across a range of technologies, advising early stage and established companies in the development, protection, and enforcement of their intellectual property rights. Mr. Zemsky is a presenter at national biotech and law conferences and has spoken on intellectual property panels as it pertains to the healthcare industry.