Current Decisions and Events Impacting IP – Recent Case Discussions and Changes Impacting Your Practice

Michael I. Chakansky, Esq. (Panel Chair)
Hoffmann & Baron, LLP, Parsippany, NJ

Marc A. Lieberstein, Esq.
Kilpatrick Townsend & Stockton LLP, NYC

Rory J. Radding, Esq.
Locke Lorde LLP, NYC

Victoria Cundiff, Esq.
Paul Hastings Janofsky & Walker, LLP, NYC

Richard L. Ravin, Esq.
Hartman & Winnicki, PC, Ridgewood, NJ

Paul M. Fakler, Esq.
Arent Fox LLP, NYC

Kelly Slavitt, Esq.
Reckitt Benckiser LL, Parsippany, NJ

Michael I. Chakansky
Hoffmann & Baron, LLP
6 Campus Drive
Parsippany, NJ 07054
973.331.1700
mchakansky@hbiplaw.com

Past-Chair Intellectual Property Law Section 1998-2000

THIRTY FIVE YEARS OF CHANGES IN PATENT LAW

As a patent attorney practicing for over 35 years, I can say without equivocation that the patent landscape has changed significantly since my admission as a patent attorney, which coincidentally was also the year the Court of Appeals for the Federal Circuit came into existence.

During that time, issued patents were first subjected to review: starting with *ex parte* reexamination, then adding *inter partes* reexamination (now discontinued), and finally adding the AIA post grant trifecta of *inter partes* review (IPR), post grant reviews (PGR) and covered business method review (CBM). The U.S. went from a first to invent to a first inventor to file system. Patents were now subject to invalidity claims at the US Patent and Trademark Office (PTO). Utility patent terms went from 17 years from issuance (without any maintenance fees) to generally 20 years from the effective filing date (though currently the term may be extended to compensate for delay from PTO/FDA review) and periodic maintenance fees payments to the PTO are required to keep the patent alive.

When I started laches was available to the defendant within the 6 year damages period before the filing of a complaint. Now, laches are unavailable during that 6 year damages period. Back when I started, a written patent opinion was generally necessary to defeat a claim a of willful patent infringement, it is no longer necessary. Once the court/jury found infringement of a not-invalid patent was established, irreparable injury was presumed for injunction purposes, no longer is that the case. Once the sale of a product covered by a process patent was not a direct infringement of a process patent, now it is. Thirty-five years ago, U.S. patent applications were not published, only the issued patent was published, now non-provisional applications are published. And by the way, thirty-five years ago U.S. provisional patent applications did not exist. Filing a complaint for patent infringement was as easy as filling out Form 18, now it must meet the requirements of *Twombly* and *Igbal*. And the list goes on . . . .[1]

SELECTED RECENT AND PENDING DECISIONS

[1] Some things do not change. Thirty-five years ago there was disagreement as to the scope of patentable subject matter under § 101, today there still is.

Patent Venue is *Sui Generis*.

28 U.S.C. §1400

(b) 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.

TC Heartland v. Kraft Food (2017): For purposes of the patent venue statute, a corporation only "resides" in its state of incorporation.

In re Cray, Inc., September 21, 2017, the Federal Circuit laid out three requirements for "a regular and established place of business:" "(1) there must be a physical place in the district; (2) it must be a regular and established place of business; and (3) it must be the place of the defendant.

No laches during patent damages period.

SCA Hygiene Products v. First Quality Baby Products (2017)

Laches does not bar a claim for patent infringement brought within the Patent Act's six-year statutory limitations period, 35 U.S.C. § 286.

BRI standard applicable to post grant reviews at PTAB.

Cuozzo Speed Technologies v. Lee (2016)

The PTAB may construe claims in an issued patent according to their broadest reasonable interpretation rather than their plain and ordinary meaning.

Burden is not on Patent Owner to show that Amended Claims are patentable.

Aqua Products, Inc. v. Matal, 872 F.3d 1290 (Fed. Cir. 2017) ("The only legal conclusions that support and define the judgment of the court are: (1) the PTO has not adopted a rule placing the burden of persuasion with respect to the patentability of amended claims on the patent owner that is entitled to deference; and (2) in the absence of anything that might be entitled deference, the PTO may not place that burden on the patentee.")

On November 21, 2017, the PTAB issued guidance on claim amendment in post grant reviews in view of *Aqua Products*. In part (emphasis supplied):

> In light of the *Aqua Products* decision, the Board will not place the burden of persuasion on a patent owner with respect to the patentability of substitute claims presented in a motion to amend. Rather, if a patent owner files a motion to amend (or has one pending) and that motion meets the requirements of 35 U.S.C. § 316(d) (i.e., proposes a reasonable number of substitute claims, and the substitute claims do not enlarge scope of the original claims of the patent or introduce new matter), the Board will proceed to determine whether the substitute claims are unpatentable by a preponderance of the evidence based on the entirety of the record, including any opposition made by the petitioner. *Thus, for example, if the entirety of the evidence of record before the Board is in equipoise as to the unpatentability of one or more substitute claims, the Board will grant the motion to amend with respect to such claims, and the Office will issue a certificate incorporating those claims into the patent at issue*.

Is Post Grant Review Constitutional?

Oil States Energy Services v. Greene's Energy Group (argued Nov. 27, 2017).

> Whether *inter partes* review-an adversarial process used by the Patent and Trademark Office (PTO) to analyze the validity of existing patents- violates the Constitution by extinguishing private property rights through a non-Article III forum without a jury.

Does the PTAB have to address all claims in its Post Grant Review?

SAS Institute Inc. v. Matal (argued Nov. 27, 2017).

> Does 35 U.S.C. § 318(a), which provides that the Patent Trial and Appeal Board in an *inter partes* review "shall issue a final written decision with respect to the patentability of any patent claim challenged by the petitioner," require that Board to issue a final written decision as to every claim challenged by the petitioner, or does it allow that Board to issue a final written decision with respect to the patentability of only some of the patent claims challenged by the petitioner, as the Federal Circuit held?

LOCKE LORD® QUICK Study
Trademark, Copyright and Advertising Practice

Opening Trademarks to New Possibilities -- Federal Circuit Affords Immoral or Scandalous Trademarks First Amendment Protection

By: Rory J. Radding and Scott D. Greenberg

After the Trademark Office refusing registration for immoral or scandalous marks over the past 100 years, the U.S. Court of Appeals for the Federal Circuit recently held that the provision of Section 2(a) of the U.S. Trademark Act (15 U.S.C. §1052(a)) authorizing refusal of registration of trademarks that comprise immoral or scandalous matter is an unconstitutional restriction of the right of free speech under the First Amendment. *In re Brunetti*, case no. 2015-1109, slip op. (Fed. Cir. December 15, 2017). This decision follows on the heels of *Mattal v. Tam*, 137 S.Ct. 1744 (2017), in which the Supreme Court affirmed the Federal Circuit's *en banc* opinion that another refusal provision of Section 2(a), namely the refusal on the ground that the mark may be disparaging to persons living or dead, institutions or beliefs, also violated the First Amendment right of free speech. As further discussed below, *Brunetti's* invalidation of the immoral/scandalous ground for refusing registration of a trademark likely will have greater impact than *Tam's* elimination of the "disparaging" refusal.

The Federal Circuit's Decision

Brunetti involved an application to register the trademark "FUCT" in connection with clothing products. The Examining Attorney in the U.S. Patent and Trademark Office refused registration under Section 2(a) on immoral/scandalous grounds, and this refusal was affirmed by the USPTO's Trademark Trial and Appeal Board. On further appeal to the Federal Circuit, the Court agreed that the mark at issue was immoral or scandalous under the statute, essentially because the mark would be considered "vulgar" by a substantial portion of the general public, taking into account contemporary attitudes. Slip op. at 3. However, the Court went on to hold that refusing to register trademarks because they are vulgar is an improper governmental restriction of free speech.

The Court noted that a statute is presumptively invalid under the First Amendment if it restricts, or has a chilling effect upon, speech based on content, specifically, when "a law applies to particular speech because of the topic discussed or the idea or message expressed." Slip op. at 13. The government can overcome this presumption of invalidity by demonstrating that the statute either (a) constitutes a type of government activity which does not implicate the First Amendment, e.g. a government subsidy program or the provision of a limited public forum, (b) survives "strict scrutiny" review, i.e. "that the restriction furthers a compelling interest and is narrowly tailored to achieve that interest" (slip op. at 13), or (c) only regulates commercial speech and survives the "intermediate scrutiny" review standard, i.e. that the statute "directly advances a substantial government interest and that the measure is drawn to achieve that interest" (slip op. at 28).

In *Brunetti*, the Government conceded that the immoral/scandalous refusal is a content-based restriction on speech that would not survive strict scrutiny review. Slip op. at 13. However, the Government contended that the federal trademark registration system (a) constitutes either a government subsidy or a limited public forum, or (b) alternatively, only regulates commercial speech and the immoral/scandalous refusal survives intermediate scrutiny.

The Court rejected all of the Government's contentions. The trademark registration system was held not to constitute a government spending program of the type that might give rise to the "subsidy" exception, because the trademark applicant is not receiving federal funds when the USPTO grants a trademark registration (slip op. at 17). The registration system is not a limited public forum, i.e. a situation in which "the government has opened its property for a limited purpose" (slip op. at 21), because trademarks exist in the marketplace, and "the speech that flows from trademark registration is not tethered to…any…government property" (slip op. at 24). The register of trademarks is merely a database and not a forum for the exchange of ideas. Slip op. at 25.

Finally, the commercial speech/intermediate scrutiny contention was rejected, with the Court holding that the immoral/scandalous refusal (1) targets the expressive content of marks and not their commercial function, and (2) in any event, the desire to protect "the public from off-putting marks is an inadequate government interest for First Amendment purposes." Slip op. at 26 – 34.

The Federal Circuit also held that it would not be proper judicial conduct for the Court to construe the immoral/scandalous refusal as only applying to "obscene" marks, in order to avoid the issue of constitutionality, because such a limitation was not a reasonable or foreseeable interpretation of the wording of the statute.

Possible Further Proceedings

It is possible that the Government may seek further review of the *Brunetti* decision, either by way of *en banc* review by the Federal Circuit and/or review by the Supreme Court. However, as noted above, earlier this year the Supreme Court, in the *Tam* case, affirmed the Federal Circuit's *en banc* opinion holding that the "disparaging" ground of refusal in Section 2(a) of the Trademark Act also violated the First Amendment right of free speech. The Supreme Court and Federal Circuit decisions in Tam would probably render it difficult for the Government to obtain a reversal of the *Brunetti* decision at either level.

Potential Impact

Assuming that the Federal Circuit's holding in *Brunetti* becomes completely final, i.e. if all potential avenues of review are exhausted without any change in the outcome, the USPTO will probably issue a formal policy statement confirming that the "immoral/scandalous" provision of the statute is no longer a valid ground for refusing registration (a similar statement was issued with respect to the "disparaging" ground of refusal following the Supreme Court's decision in *Tam*).

However, it is possible that *Brunetti's* overturning of the "immoral/scandalous" ground of refusal may have even greater impact than Tam's overturning of the "disparaging" refusal.

As noted above, the "immoral/scandalous" ground applies to marks consisting of words or images that would be considered "vulgar" by a substantial portion of the general public, taking into account contemporary attitudes. It has been observed that the use of such crude or vulgar language and imagery is a growing trend within the marketing and advertising of consumer goods and services, where the use of such content may be deemed an effective marketing strategy based on the nature of the products and the demographics of the targeted audience. For example, in the case of products and services that appeal to relatively younger consumers, and for which social media marketing is an important tool, there is often a motivation to employ "edgy" advertising techniques including crudity. *See, e.g.,* Stuart Elliott, *Crude? So what? These characters still find work in ads*, N.Y. Times, June 18, 2008, at C9. To the extent that the makers and sellers of such consumer products and services are inclined, for similar reasons, to adopt *marks* which are crude or vulgar, such an inclination will no doubt only be enhanced knowing that such marks can receive a full panel of protection including federal registration.

On the other hand, the marks that were impacted by *Tam* are those that are disparaging to groups of persons or beliefs. It has been observed that the use of such disparaging content in advertising and marketing is increasingly being perceived as crossing a line, with negative consequences for the

advertiser. See *Stuart Elliott and Tanzina Vega, Trying to Be Hip and Edgy, Ads Become Offensive*, N.Y. Times, May 11, 2013, at B1. Therefore, while marks which disparage in this way are also now registrable, many makers and sellers of consumer products and services may be more likely to exercise self-restraint and refrain from adopting such marks, notwithstanding the availability of federal registration.

Take Away Lesson

Now that immoral or scandalous marks are registrable, companies seeking to establish an "edgy" brand or provide shock value so that their brand stands out, may do so with the added assurance that the "edgy" mark will be enforced under federal law, without regard to the sensibilities of a substantial portion of the general public.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact the authors.

Rory J. Radding | 212-912-2858 | rory.radding@lockelord.com
Scott D. Greenberg | 212-415-8512 | sgreenberg@lockelord.com

Rock On! In Florida, Pre-1972 Sound Recordings are Fair Game for Music Services

Paul Fakler and Margaret Wheeler-Frothingham

On October 26, the Florida Supreme Court issued a decision in *Flo & Eddie, Inc. v. Sirius XM Radio, Inc.*, Case No. SC16-1161, holding that Florida's common law copyright does not recognize any public performance right for sound recordings made prior to 1972. This ruling, which echoes a similar decision by New York's highest appellate court in December of 2016, is the second consecutive appellate win for the broadcast and webcasting industries arising out of a series of similar state law copyright infringement cases filed throughout the country by Flo and Eddie of the Turtles, and is an important step towards resolving ongoing legal debates over the royalty obligations of services using sound recordings from the golden era of rock and roll.

Sound recordings created before 1972 are not protected under federal copyright law. "Musical works" – the underlying musical compositions performed in those recordings – have enjoyed federal copyright protection since 1831. In 1909, Congress expanded federal copyright protection for musical compositions to include an exclusive public performance right. It was not until 1971 that Congress extended any federal copyright protection to the *recordings* of those musical works. This protection took effect only for sound recordings created on or after February 15, 1972, and did not include any public performance right so that music users such as broadcasters would not be disrupted by a new royalty obligation. At that time, Congress made clear that the new prospective sound recording copyright did not preempt any state law protections for pre-1972 sound recordings. In 1995, Congress expanded federal protection for post-1972 sound recordings, creating a limited public performance right for digital audio transmissions only. Terrestrial AM/FM radio broadcasters still pay no royalties for the public

performance of sound recordings (although they do pay public performance royalties for the underlying musical compositions).

Flo & Eddie, Inc. ("Flo & Eddie"), the appellant in this case, owns the master sound recordings of various musical performances recorded by the rock band The Turtles prior to 1972. SiriusXM had played the Turtles' pre-1972 recordings on its satellite and internet radio services – a use which Flo & Eddie had never expressly licensed and for which it received no royalties. Flo & Eddie brought suits against SiriusXM in Florida, New York, and California, asserting that it had the exclusive right of public performance in its pre-1972 sound recordings under the laws of each state and that SiriusXM had violated that right, that SiriusXM's use of buffer copies violated the exclusive reproduction right under the common law of those states, and various other state law claims based upon the alleged violations of its state law copyrights. In December of 2016, New York's highest appellate court rejected Flo & Eddie's claims and found for SiriusXM. Last week, the Florida Supreme Court issued a similar decision.

In Florida, the case was first ruled upon by a federal district court, which agreed with SiriusXM that Florida did not recognize any common law right of public performance for pre-1972 sound recordings. On appeal, the Eleventh Circuit, recognizing a dearth of Florida case law addressing whether Florida recognized a common law copyright in sound recordings, certified the pending questions of Florida law to the Florida Supreme Court. Following a review of the statutory and common law treatment of sound recordings under Florida law, the Florida court reached the ultimate conclusion that "Florida common law does not recognize an exclusive right

of public performance in pre-1972 sound recordings," and that to do so for the first time would be a legislative, not a judicial task.

The court noted that Flo & Eddie had sought an "unfettered" right of public performance for pre-1972 sound recordings – one far broader than the "carefully delineated" right the Congress has recognized for the public performance of post-1972 sound recordings. The court staunchly declined to reach the conclusion that "Congress eventually granted a right in 1972 that was significantly less valuable than the right Flo & Eddie claims has existed all along under the common law in Florida and elsewhere." Instead, the court found that Florida common law has never recognized an exclusive right of public performance in pre-1972 sound recordings,

Practical considerations and concerns about market disruption underpinned the court's decision: the opinion noted that recognizing a public performance right in pre-1972 sound recordings would have an immediate impact on consumers and businesses beyond Florida, including stakeholders not party to the case. The district court in the Florida case, and the New York court, had echoed similar concerns in their decisions.

The Florida court also rejected Flo & Eddie's claims that SiriusXM's use of "buffer copies" in the transmission of its broadcast violated any post-sale exclusive right of reproduction, agreeing with the Second Circuit that the use of such intermediate copies for the purpose of making otherwise lawful performances is permissible under copyright law. Having rejected Flo & Eddie's claim that a common law property rights existed and were violated, the court found

that Flo & Eddie's remaining state law claims, all of which were predicated upon the alleged common law copyright violations, also failed.

This decision reinforces the status quo, avoiding a potential upset of the licensing practices of nationwide broadcasters and digital music services. The final outcome of the Flo & Eddie litigation strategy now hinges on the appellate decision in the pending California case. If the California case were to reach a different conclusion than those in Florida and New York, the music broadcasting industries would have two poor choices. Music services could attempt to implement a complex licensing scheme, applying different licensing practices to different states and seeking licenses from thousands of different record companies. Alternatively, services could attempt to program their music channels and stations differently for listeners located in different states, based upon each state's recognition of pre-1972 performance rights. Unless and until that happens, however, broadcasters and webcasters can breathe a sigh of relief and continue to play those great 60's hits on their services.

2018 Annual Meeting
Of The
Intellectual Property Law Section

Recent Developments and Important Topics in Internet Law

Presented by
Richard L. Ravin, Esq.,
Chair of Internet and Technology Law Committee, and
Past Chair, Intellectual Property Law Section,
New York State Bar Association

January 23, 2018
New York Hilton
New York City

By: Richard L. Ravin, Esq.
Hartman & Winnicki, P.C.
Counselors At Law
74 Passaic Street
Ridgewood, NJ 07450
Phone: 201-9678040
E-Mail: Rick@Ravin.com
Website: www.Ravin.com

*These material are for general information purposes and is not intended to be and should not be taken as legal advice. The opinions expressed are those of the author and do not necessarily reflect the views of his firms or clients.

.

Recent Developments and Important Topics in Internet Law

- **Manipulation/Synthesis of Audio and Visual Images of People**
- **End of Net Neutrality?**
- **Driverless Cars and the Internet of Things**
- **Uniform Access to Digital Assets Law**
- **European Union's New Data Protection Regulation**
- **Taxes on Internet Sales**
- **Consumer Data Privacy Laws**
- **Websites Compliance with ADA**
- **Anti-SLAPP Suits**
- **Trademark Infringement in SEO**
- **Defamation on the Internet**
- **Communications Decency Act**
- **Stored Communications Act**
- **Cloud Computing**

- # Manipulation/Synthesis of Audio and Visual Images of People

The future of fake news: don't believe everything you read, see or hear ...

https://www.theguardian.com/.../fake-news-obama-video-trump-face2face-doctored-c...

Jul 26, 2017 - A new breed of **video** and audio **manipulation** tools allow for the creation of realistic looking news footage, like the now infamous fake Obama speech.

Video and audio manipulation tools can create artificial intelligence and computer graphics, that will allow for the creation of realistic looking footage of public figures appearing to say things they never said.

Future of fake news. Researchers working on capturing and synthesizing different visual and audio elements of human behavior.

Software developed at Stanford University is able to manipulate video footage of public figures to allow a second person to put words in their mouth – in real time.

Face2Face captures the second person's facial expressions as they talk into a webcam and then morphs those movements directly onto the face of the person in the original video.

Researchers created technology by puppeteering videos of George W Bush, Vladimir Putin and Donald Trump. It's very hard to distinguish the synthesized version from the real footage

University of Alabama at Birmingham researchers have been developing voice impersonation using only 3-5 minutes of audio of a victim's voice, which can be taken live or from YouTube

videos. Researches can create a synthesized voice that can be believe by humans and not be detected by biometric security systems, including those employed by banks and smartphones. Voice manipulation can be used with face manipulation to make convincing false statements by public officials.

University of Washington's Synthesizing Obama project: they took the audio from one of Obama's speeches and used it to animate his face in an entirely different video with incredible accuracy which is achieved by training a recurrent neural network with hours of video.

According to Nitesh Saxena, associate professor and research director of the University of Alabama at Birmingham's department of computer science. "You could leave fake voice messages posing as someone's mum. Or defame someone and post the audio samples online."

The mistrust in the news media and social media is at a high point, and the proliferation of hoaxes and false news via social media, make it even more important for news organizations to check content to make sure it is authentic.

Synthesized content posted to social media can be distributed virally in a matter of minutes, and cause a public relations, political or diplomatic tragedy. Imagine what would happen if a fake Trump speech were to declare war on North Korea

Source: The Guardian, Olivia Solon in San Francisco

The ability to **manipulate video images**. Sub-power of Recording Manipulation. Variation of Data Manipulation.

Also Called

- Electronic Medium Control/Domination/Manipulation

- Video Control/Domination
- Vínteokinesis

Capabilities

The user can create, shape and manipulate video images, allowing them to create energy constructs in shape of beings, tools, weapons, aspects of fantasy (such as an NPC, a person from a movie, etc.), and to use powers used in videos like turning invisible and summon mighty weapons. They may also develop the ability to become Digital energy and travel through electronics, wires etc. in video form.

http://powerlisting.wikia.com/wiki/Recording_Manipulation

New Digital Face Manipulation Means You Can't Trust Video Anymore
https://singularityhub.com/.../new-digital-face-manipulation-means-you-cant-trust-vid...

1.
2.

May 13, 2016 - What if you could alter a video of anyone to emulate facial and mouth movements that never existed in the source video—by yourself, at home, using a cheap webcam? Meet Face2Face. Using RGB input from one video and mapped pixels from a second **video**, **manipulating** someone's face—including ...

Scarily convincing fake video tool puts words in Obama's mouth
www.telegraph.co.uk › Technology

1.

Jul 12, 2017 - The tool could be used to **manipulate videos** to create realistic-looking fake clips. But it can only put audio spoken by a person into their mouth. "You can't just take anyone's voice and turn it into an Obama **video**," said Seitz. "We very consciously decided against going down the path of putting other people's ...

Watch a man manipulate George Bush's face in real time - The Verge
https://www.theverge.com/2016/3/.../facial-transfer-donald-trump-geoe-bush-video

1.

Mar 21, 2016 - You know that scene in the classic film Bruce Almighty when Jim Carrey uses his God-like powers to mess with Steve Carrell's character while he's giving a live news broadcast? That's what this **video** looks like (kind of), except replace Steve Carrell for George W. Bush, Donald Trump, Vladimir Putin, and ...

Smart Technologies and the End(s) of Law
Mireille Hildebrandt

This timely book tells the story of the smart technologies that reconstruct our world, by provoking their most salient functionality: the prediction and preemption of our day-to-day activities, preferences, health and credit risks, criminal intent and spending capacity. Mireille Hildebrandt claims that we are in transit between an

information society and a data-driven society, which has far reaching consequences for the world we depend on. She highlights how the pervasive employment of machine-learning technologies that inform so-called 'data-driven agency' threaten privacy, identity, autonomy, non-discrimination, due process and the presumption of innocence. The author argues how smart technologies undermine, reconfigure and overrule the ends of the law in a constitutional democracy, jeopardizing law as an instrument of justice, legal certainty and the public good. Finally, the book calls on lawyers, computer scientists and civil society not to reject smart technologies, explaining how further engaging these technologies may help to reinvent the effective protection of the rule of law. Learn More

- **End Of Net Neutrality?**

The Federal Communications Commission, under the direction of Donald Trump, has repealed the regulation that banned internet service providers from interfering with what people see on the internet and how easy it is to view. Chairman Arjit Pai, who was appointed by Mr Trump, said that the protections stopped internet companies from doing what they wanted and were an unnecessary restriction.

As such, it violates a principle that has been in place ever since the internet began: that no particular website or service can receive special treatment from the companies that power the web. Instead, service providers will be allowed to charge websites to load quicker, for instance, or force their users to pay extra if they want to access certain pages.

SOURCE: THE INDEPENDENT, BY ANDREW GRIFFIN
@_andrew_griffin Tuesday 21 November 2017 16:42 GMT
http://www.independent.co.uk/life-style/gadgets-and-tech/news/trump-net-neutrality-repeal-internet-rules-fcc-free-latest-news-ajit-pai-a8067811.html

- **New York's Uniform Access to Digital Assets Law**

In 2015, The Uniform Law Commission finalized and passed the Fiduciary Access to Digital Assets Act. New York enacted its version of the law, which took effect on September 29,

2016, amending the Estate, Powers and Trusts Laws ("EPTL") by adding new Article 13-A. It is noted, however, that EPTL Article 13-A does not have a short title, so it technically is not titled the Fiduciary Access To Digital Assets Act even though, with minor exceptions, it is identical in substance to the Uniform Law version.

Under the Uniform Law, a fiduciary is a person appointed to manage the property of another person, subject to strict duties to act in the other person's best interest. Common types of fiduciaries include executors of a decedent's estate, trustees, conservators, and agents under a power of attorney. The purpose of the legislation is to facilitate fiduciary access to digital assets, while respecting the privacy and intent of the account holder and to provide the fiduciary with the ability to administer the account holder's digital assets.[1]

The Act provides for basically four types of fiduciary relationships: (i) the personal representative (the executor or administrator) of a decedent's estate, (ii) a guardian of a ward or protected person, (iii) agents acting pursuant to a power of attorney, and (iv) trustees.

Below is a Summary by the Uniform Law Commission of the Revised Uniform Fiduciary Access to Digital Assets Act:[2]

A Summary Of The Uniform Access to Digital Assets Act

In the Internet age, the nature of property and our methods of communication have changed dramatically. A generation ago, a human being delivered our mail, photos were kept in

[1] Memo: *Proposed Legislation For The Administration Of Digital Assets*
By Joint Subcommittee For The Administration Of Digital Assets
Executive Committee, Trusts And Estates Law Section, New York State Bar Association, Trusts, Estates And Surrogates Court Committee Of The New York City Bar Association, dated October 7, 2014 ("NYSBA Memo").

[2] http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/Revised%202015/Revised%20UFADAA%20-%20Summary%20-%20Sep%202017.pdf

albums, documents in file cabinets, and money on deposit at the corner bank. For most people today, at least some of their property and communications are stored as data on a computer server and accessed via the Internet.

Collectively, a person's digital property and electronic communications are referred to as "digital assets" and the companies that store those assets on their servers are called "custodians." Access to digital assets is usually governed by a terms-of-service agreement rather than by property law. This creates problems when Internet users die or otherwise lose the ability to manage their own digital assets.

A fiduciary is a trusted person with the legal authority to manage another's property, and the duty to act in that person's best interest. The Revised Uniform Fiduciary Access to Digital Assets Act (Revised UFADAA) addresses four common types of fiduciaries:

1. Executors or administrators of deceased persons' estates;

2. Court-appointed guardians or conservators of protected persons' estates;

3. Agents appointed under powers of attorney; and

4. Trustees. Revised UFADAA gives Internet users the power to plan for the management and disposition of their digital assets in a similar way as they can make plans for their tangible property. In case of conflicting instructions, the act provides a three-tiered system of priorities:

1. If the custodian provides an online tool, separate from the general terms of service, that allows the user to name another person to have access to the user's digital assets or to direct the

custodian to delete the user's digital assets, Revised UFADAA makes the user's online instructions legally enforceable.

2. If the custodian does not provide an online planning option, or if the user declines to use the online tool provided, the user may give legally enforceable directions for the disposition of digital assets in a will, trust, power of attorney, or other written record.

3. If the user has not provided any direction, either online or in a traditional estate plan, the terms of service for the user's account will determine whether a fiduciary may access the user's digital assets. If the terms of service do not address fiduciary access, the default rules of Revised UFADAA will apply.

Revised UFADAA's default rules attempt to balance the user's privacy interest with the fiduciary's need for access by making a distinction between the "content of electronic communications," the "catalogue of electronic communications", and other types of digital assets.

The content of electronic communications includes the subject line and body of a user's email messages, text messages, and other messages between private parties. A fiduciary may never access the content of electronic communications without the user's consent. When necessary, a fiduciary may have a right to access a catalogue of the user's electronic communications – essentially a list of communications showing the addresses of the sender and recipient, and the date and time the message was sent.

For example, the executor of a decedent's estate may need to access a catalogue of the decedent's communications in order to compile an inventory of estate assets. If the executor finds that the decedent received a monthly email message from a particular bank or credit card

company, the executor can contact that company directly and request a statement of the decedent's account.

Other types of digital assets are not communications, but intangible personal property. For example, an agent under a power of attorney who has authority to access the principal's business files will have access under Revised UFADAA to any files stored in "the cloud" as well as those stored in file cabinets. Similarly, an executor that is distributing funds from the decedent's bank account will also have access to the decedent's virtual currency account (e.g. bitcoin).

Under Revised UFADAA Section 15, fiduciaries for digital assets are subject to the same fiduciary duties that normally apply to tangible assets. Thus, for example, an executor may not publish the decedent's confidential communications or impersonate the decedent by sending email from the decedent's account. A fiduciary's management of digital assets may also be limited by other law. For example, a fiduciary may not copy or distribute digital files in violation of copyright law, and may not exceed the user's authority under the account's terms of service.

In order to gain access to digital assets, Revised UFADAA requires a fiduciary to send a request to the custodian, accompanied by a certified copy of the document granting fiduciary authority, such as a letter of appointment, court order, or certification of trust. Custodians of digital assets that receive an apparently valid request for access are immune from any liability for acts done in good faith compliance.

Revised UFADAA is an overlay statute designed to work in conjunction with a state's existing laws on probate, guardianship, trusts, and powers of attorney. It is a vital statute for the digital age, and should be enacted by every state legislature as soon as possible.

For further information about Revised UFADAA, please contact ULC Legislative Counsel Benjamin Orzeske at 312-450-6621 or borzeske@uniformlaws.org.

Summary of by the Uniform Law Commission of the Revised Uniform Fiduciary Access to Digital Assets Act, http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/Revised%202015/Revised%20UFADAA%20-%20Summary%20-%20March%202016.pdf (accessed on October 15, 2017).

Will It Work?

The big unknown is whether the Acts enacted around the country will achieve their goal. The impediment is federal law and the preemption doctrine. Basically, the Stored Communication Act (SCS), discussed below, makes disclosure of the stored communication voluntary on the part of the remote computing service (i.e., online service providers, such as, Google, Facebook, Twitter, Instagram, Amazon). The simple solution would be for Congress to expressly amend the SCA to make it mandatory for the remote computing services to abide by the requests of fiduciaries to access the digital assets of their decedents, wards, principals and trusts. Even with enactment of these comprehensive laws, the remote computing services will likely argue that compliance with the fiduciary access laws is still discretionary, or, even worse, that access is prohibited. This is because the SCA does not expressly recognize representatives of the originator, user or account holder as having the same rights to access as the originator, user, or account holder himself, herself or itself. Nonetheless, the laws are a step in the right direction and they would give "cover" to a remote computing service that was inclined to comply with the requests of fiduciaries.

Current Law Impacting Access By Fiduciaries to Digital Assets[3]

Federal laws criminalize, or penalize, the **unauthorized access of computers and digital accounts** and prohibit most service providers from disclosing account information to anyone without the account holder's consent. These laws include the Electronic Communications Privacy Act (the "ECPA")[4], the Stored Communications Act (the "SCA")[5], which is part of the ECPA, and the Computer Fraud and Abuse Act (the "CFAA").[6] The CFAA prohibits unauthorized access to computers and protects against anyone who "intentionally accesses a computer without authorization or exceeds authorized access."[7]

Title I of the ECPA protects wire, oral, and electronic communications **while in transit**, e.g., requiring search warrants from law enforcement for disclosures (18 U.S.C. § 2510 et seq.). Title II of ECPA (SCA) protects communications which are **in electronic storage**, with less protection than those of Title I, e.g., not requiring warrants for disclosure. However, under SCA, disclosure is voluntary. While the online service provider ("remote computing service", defined by the SCA) may require that it be served with a subpoena prior to disclosure of communications, such service providers have argued and will continue to argue that disclosure cannot be compelled by a court. It is noted that the law does not require that a subpoena be served in order that the remote computing service is allowed to disclose the information – this is a self-created rule of the remote computing services.

Remote computing service[s] [8] do consider data (and, e.g. pictures, documents of any kind, etc.) as such, and routinely refuse disclosure of any such thing which was an "electronic

---

[3] See, NYSBA Memo.
[4] 18 U.S.C. § 2510 *et seq*. (2006).
[5] 18 U.S.C. § 2701 *et seq*. (2006).
[6] 18 U.S.C. § 1030 *et seq*. (2006).
[7] 18 U.S.C. § 1030(a).
[8] 18 U.S.C. § 2711 (2).

transmission".[9] Although, electronic transmission is not defined in the SCA, it is used in conjunction with other terms, such as the definition of "electronic storage" (defined, in part as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof….)[10]. Whether the logic of the remote computing services as to their broad interpretation of "electronic communications" will withstand judicial scrutiny remains to be seen. However, for now they, and their logic, are forces to be reckoned with.

The SCA contains two relevant prohibitions. First, the SCA makes it a crime for anyone to "intentionally access without authorization a facility through which an electronic communication service is provided"[11] as well as to "intentionally exceed an authorization to access that facility."[12] Second, the SCA prohibits an electronic communications service from knowingly divulging the contents of a communication that is stored by or maintained on that service unless disclosure is made "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient" or "with the lawful consent of the originator or an addressee or intended recipient of such communication, ..."[13] The SCA is often the basis on which service providers refuse to release the contents of a deceased user's account. [14]

---

[9] The definitions of Title I of the ECPA (18 U.S.C. § 2510) are made applicable to the SCA by 18 U.S.C. 2711(1).
[10] 18 U.S.C. § 2510(17).
[11] 18 U.S.C. § 2701(a).
[12] Id.
[13]18 U.S.C. § 2702(b)(1) and (3).

[14]*See* e.g., *In re Facebook, Inc*. (In December 2008, 23 year-old Sahar Daftary fell twelve floors to her death from her estranged husband's flat in England. The local authorities determined that Daftary's death was likely a suicide. The family, however, disputed that determination and believed that the contents of her Facebook account contained critical evidence showing her state of mind in the days leading up to her death. Because Daftary died in England, a local probate court was not available, so the family turned to the federal district court in California (where Facebook corporate headquarters is located) to order Facebook to disclose the contents of Daftary's account. The district court granted Facebook's motion to quash the subpoena stating that to hold otherwise would "run afoul of the 'specific [privacy] interests that the [SCA] seeks to protect.'" Regarding the alleged consent given by family members on behalf of Daftary, the court stated that under the "plain language of Section 2702 [of the SCA], while consent may *permit* production by a provider, it may not *require* such a production." The court, in dicta, stated that Facebook

Importantly, disclosure of contents of communications by the remote computing service, while permitted, is discretionary.

The Federal Communications Act of 1934, as amended, 47 U.S. §151 et seq., also has a provision that protects customer information.[15]

In addition to federal privacy laws, state privacy laws must also be considered. All 50 states, including New York have enacted criminal laws penalizing unauthorized access to computer systems.[16]

Consequently, with the prohibitions contained in the federal and state privacy laws, many service providers have and may continue to refuse to provide access or release content upon the death or incapacity of an account holder for fear of facing certain liability. Importantly, online service providers may further protect themselves by requiring an account holder to agree to a Terms of Service ("TOS") agreement prior to creating an online account, which would be binding on representatives, agents and fiduciaries of the account holder.

In the absence of laws dealing with the disposition of digital assets, individuals will be subject to the service provider's TOS if the TOS has a policy regarding the transfer or disposal of account access and content. Some service providers have a policy that indicates what will

---

could on its own determine that family members could provide consent on behalf of Daftary and release the information. To date, Facebook has not provided such access).

[15] 47 U.S. Code § 222 - Privacy of customer information.

[16] S*ee e.g.* **New York Penal Code 156.00** et seq**. Offenses involving Computers. *N.J.S.A.* 2C:20-25 Computer criminal activity;** CAL. PENAL CODE § 502 (2010); FLA. STAT. ANN. § 815.06 (2013); 720 ILL.

happen upon the death of an account holder. [17] Others have no explicit policy. [18] Some may elect that the data be deleted or some or all of it may be sent to a specified individual.

- ## Driverless Cars and the Internet of Things

The following article, "Legal Developments in Connected Car Arena Provide Glimpse of Privacy and Data Security Regulation in Internet of Things", by F. Paul Pittman, is reprinted here with permission from its author, Mr. Pittman.

[17] http://support.google.com/mail/answer/14300?hl=en&ref_topic=1669055 (website last checked May 2014). Gmail has a policy for potentially releasing emails to the personal representative of a deceased account holder. The policy makes it clear, however, that a court order will be required and there is no guarantee the email content will be released. Google, however, became the first service provider to implement a solution regarding access to a user's account upon his or her death or incapacity. The Inactive Account Manager will become "activated" after the user's account is inactive for a period of three, six, nine or twelve months, as determined by the user. The user can also determine what will happen to his or her data in advance of the account becoming inactive. For instance, the user .

[18] See e.g., http://www.shutterfly.com/help/terms.jsp; http://www.linkedin.com/static?key=user_agreement&trk=hb_ft_userag; http://www.google.com/intl/en/policies/terms/; https://twitter.com/TOS (each website last checked May 2014). Shutterfly's TOS does not include an explicit discussion of what happens when the account holder dies. Shutterfly's TOS states that the individual agrees not to disclose his or her username or password to any third party and acknowledges that the individual's access to the account is non-transferable. LinkedIn and Google have similar policies.

Legal Developments in Connected Car Arena Provide Glimpse of Privacy and Data Security Regulation in Internet of Things

By F. Paul Pittman*

February 2, 2016

*The author may be contacted at Paul.Pittman@whitecase.com

With the holiday season in the rear view, automobiles equipped with the newest technology connecting carmakers with their vehicles, vehicles with the world around them, and drivers with the consumer marketplace – Connected Cars – have moved from the lots to driveways. Automakers are remaking their fleets to offer unprecedented choice and convenience to drivers. However, as recent studies have shown, the connectivity inherent in Connected Cars, and the fast pace at which the industry is developing, raise privacy, data security, and physical safety concerns about the vulnerability of Connected Car computer systems. Lawmakers and regulators have begun to devote increased attention to this issue while plaintiffs' attorneys have been emboldened to haul automakers, manufacturers, and computer system developers into court. As one of the earliest entrants into and faster-growing components of the Internet of Things (IoT), Connected Cars represent a testing ground for the development of consumer privacy rights and security standards for the IoT. The approach by Congress and the courts to the governance of Connected Cars will likely guide the development of standards and practices across the IoT spectrum.

Internet of Things

Connected Cars are part of the growing and evolving Internet of Things. The IoT describes the ecosystem of everyday products and services that are equipped with "smart" technology that allows them to connect to other products or services to communicate and transfer information about users to retailers, manufacturers, and the like, typically via a wireless network. The IoT currently includes devices we use every day such as Fitbits, connected appliances, smartphones and smart TVs. As the industry grows, IoT devices will continue to permeate the objects we use on a daily basis.

Connected Cars in particular will compose the majority of the automotive fleet in the near future. The market for Connected Cars is projected to reach $54 billion in the next two years. It is estimated that by 2020 there will be 250 million Connected Cars on the road, and about 90 percent of new vehicles in Western Europe will be connected to the Internet. Connected Cars provide consumers with convenience and a personalized driving experience. Automakers and retailers gain access to consumers to provide improved services and to market

products. Onboard computers allow for navigation technologies and integration with mobile devices that complement and enhance the vehicle technology. They also allow for the collection of driver data and other driver information to enable companies to efficiently deploy customized services and experiences. Automakers are developing Connected Car technology that will allow drivers to shop through the car dashboard, based on their location and preferences determined through data collection.

Connected Car Privacy and Security Vulnerabilities

The connectivity necessary for providing the features offered by Connected Cars may pose privacy and security dangers and vulnerabilities. Connected Cars can contain more than 50 separate electronic control units (ECUs) connected through a controller area network (CAN) or other network. Those ECUs communicate with each other and the CAN through use of digital messages called CAN packets. If CAN packets are not authenticated or encrypted, they may be susceptible to remote hacking through the vehicles' wireless and phone components. This wireless technology may also enable unauthorized access to other systems and data collected by the vehicle, such as location data and potentially payment card data used for dashboard shopping.

There are also concerns about Connected Cars being subject to remote interference and operation. Security researchers' published findings have sparked increased industry, regulatory, and congressional interest in this area. One notable example involved a report that researchers were able to remotely access a car and change the car's air-conditioning settings, switch the volume and station on the radio, turn on the windshield wipers, and display a picture of the researchers on the digital dashboard screen from 10 miles away. The researchers also were able to disable the vehicle's engine and brakes, control the steering wheel, and track the car's GPS coordinates. The researchers claim that they could gain access to the vehicle from as far as 70 miles away.

Evolving Legal Landscape

Proposed Legislation

As manufacturers develop the vehicles and infrastructure that enable the use of Connected Cars, the legal landscape is struggling to keep up. Congress has proposed but has not enacted new legislation. On July 21, 2015, Senators Edward Markey (D-Mass.) and Richard Blumenthal (D-Conn.) proposed legislation (S. 1806) requiring the Department of Transportation's National Highway Traffic Safety Administration (NHTSA) to team with the Federal Trade Commission (FTC) to establish certain consumer data privacy and car computer network security rules to prevent hacking in all motor vehicles manufactured for sale in the U.S. ("SPY Car Act"). The SPY Car Act was based on a February 2015 report by Senator Markey, who had surveyed automakers about cybersecurity threats to safety and the collection and storage of driving data, including location, driving history, and user data. The report found that nearly all cars on the market have wireless technologies and identified several purported weaknesses in the security of connected features in cars.

The SPY Car Act would require collaboration between the NHTSA and the FTC to implement cybersecurity standards for vehicle system and driving data security, including

- hacking protection and mitigation;
- a "cyber dashboard" display label affixed to the vehicle that describes the vehicle's compliance with cybersecurity and privacy requirements under the SPY Car Act; and
- certain privacy standards including providing notice and choice regarding the use and collection of data, and limiting the use of driving data by manufacturers. Violators of the SPY Car Act cybersecurity standards would be penalized up to $5,000 per violation.

Violations of the privacy standards would be treated as unfair and deceptive acts or practices under Section 5 of the FTC Act.

In addition, in October 2015, Representatives Joe Wilson (R-S.C.) and Ted Lieu (D-Calif.) suggested legislation titled Examining Ways to Improve Vehicle and Roadway Safety: Vehicle Data Privacy that would require auto manufacturers to:

- develop and implement a privacy policy regarding the collection, sharing, and use of driver and vehicle data;
- file their privacy policies with the Secretary of Transportation;
- retain data only for legitimate business purposes; and
- implement reasonable security measures to prevent hacking. The proposed legislation would impose on auto manufacturers penalties of up to $1 million for failing to file a privacy policy or comply with an express privacy policy and fines of up to $100,000 for failing to prevent hacking.

The proposed legislation would also require the NHTSA to create an Automotive Cybersecurity Advisory Council to develop cybersecurity best practices for vehicle manufacturers.

Notably, the proposed legislation contains a safe harbor against FTC enforcement under Section 5 of the FTC Act for companies that file a privacy policy complying with these requirements. Unsurprisingly, the FTC has expressed disapproval of this provision, which could provide immunity to an auto manufacturer that does not follow its privacy policy and prohibit the FTC from enforcement actions against auto manufacturers for privacy-related misrepresentations on their websites, whether accessed through the vehicle or otherwise.

Self-Regulation

The automotive industry and even the FTC have cautioned that IoT-specific legislation may stifle IoT innovation and penalize companies that attempt to implement reasonable privacy and security measures. Many lawmakers have little understanding of the IoT and are not yet equipped to address the issues it presents.

Notably, and despite the pending proposed SPY Car Act, the Senate passed a resolution on March 24, 2015, that recognizes the importance of the development of the IoT and resolves that public and private entities should guide the strategy for advancing the technology. The resolution calls for Congress and the industry to collaborate to advance a national Internet of Things strategy that does not result in overregulation that stifles and prevents innovation and growth.

The automotive industry has also taken steps toward self-regulation. In November 2014, the Alliance of Automobile Manufacturers, Inc., and the Association of Global Automakers, Inc., published the Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services. These principles relate to the collection, use, and sharing of personal and vehicle information associated with vehicle technologies that collect, generate, record, and store this information. The principles call for automakers and manufacturers to ensure the following by 2017:

- provide consumers with clear notice and choice in the use and collection of personal information;
- use personal information in a way that is consistent with the context in which it was collected;
- collect information only as legitimately needed, and retain it for only as long as necessary;
- implement reasonable data security measures;
- maintain the accuracy of the data, and provide access to users; and
- remain accountable to consumers for adherence to these principles.

The Alliance of Automobile Manufacturers, Inc., and the Association of Global Automakers, Inc., have also formed an Information Sharing and Analysis Center (ISAC) to share intelligence about vehicle cybersecurity threats and designed a framework to further the development of automotive cybersecurity best practices on how to safeguard against and respond to threats.

Enforcement

Whether the regulatory framework surrounding Connected Cars emanates from legislation or self-regulation, several agencies are poised to take the lead in enforcement activities in the area. In fact, the SPY Car Act requires collaboration between the FTC and the NHTSA in developing privacy and security standards for Connected Cars. The FTC has traditionally been the lead regulator of consumer privacy and data security standards by using its authority under Section 5 of the FTC Act to contend that a lack of reasonable security measures or other missteps amount to unfair or deceptive acts or practices. The FTC has indicated an intent to play a similar role with regard to Connected Cars as evidenced by the guidance IoT document it issued titled Internet of Things – Security and Privacy in a Connected World. This guidance document encourages companies operating in the IoT to implement "security by design" into their products, along with providing consumers notice and choice with regard to collection and use of the personal information, and ensuring that companies' data collection and use practices are transparent and minimize data collection, among other suggested best practices.

NHTSA is a relatively new entrant into the data privacy and security enforcement arena, but it will be tasked with ensuring that automakers and manufacturers implement security standards sufficient to protect Connected Car computer systems from being accessed and physically controlled. NHTSA has published guidance on automotive cybersecurity, including application of the National Institute of Standards and Technology (NIST) Risk Management framework in the automotive cybersecurity context. And NHTSA recently completed an investigation of an auto manufacturer and its computer system vendor related to vehicle cybersecurity, which is particularly important since some technology company vendors supply these same systems to other car manufacturers. Automakers appear to be receptive to NHTSA's approach as they recently announced a data sharing safety agreement that reaffirms the commitment of NHTSA and automakers to collaborate on the development of cybersecurity best practice, and the continued sharing of information on cybersecurity threats and countermeasures to repel potential hackers. As Connected Car technology grows to encompass more products and services, the Federal Communications Commission (FCC) may also emerge as an enforcement player under its expanded enforcement authority over "telecommunications service" providers. Internet service providers that offer the wireless Internet services that fuel Connected Car connectivity could face increased scrutiny by the FCC, and potential fines, over the adequacy of their privacy practices and security standards for the collection of consumer personal information crossing their wireless networks.

Litigation

Class actions alleging claims based on privacy and security issues related to Connected Cars have already been filed. In an action filed in California federal court, the plaintiffs sought to certify a class of car owners who allege that the defendant car manufacturers created and concealed data privacy and vehicle security vulnerabilities through the continued use of the CAN system. The plaintiffs alleged that the CAN system is susceptible to being hacked, which could allow for the collection of data stored on the CAN system and for the control of certain vehicle functions such as steering, braking, and acceleration. The plaintiffs asserted claims for express and implied breach of warranty, fraud, false advertising, and violations of consumer protection laws. The plaintiffs sought injunctive relief, updates to the CAN system to secure and protect vehicles and data, and recovery of economic losses associated with the loss of their vehicles' value.

The defendant car manufacturers moved to dismiss the action, arguing that the plaintiffs did not suffer any "injury in fact" because their cars have not been hacked or taken control of, nor had their data been breached. The defendants relied primarily on *Clapper v. Amnesty Int'l,* where the Supreme Court held that to establish standing, a plaintiff must allege more than a speculative injury, but rather the injury alleged must be "concrete and particularized" and "actual or imminent." The defendants also asserted that the plaintiffs lacked standing to bring an invasion of privacy claim because the plaintiffs did not have a reasonable expectation in the privacy of the personal data collected by the Connected Car and that the type of data collected did not cause a "serious invasion of privacy." The plaintiffs claimed that they had been injured by the defendant car manufacturers' alleged misrepresentations about the alleged privacy and security defects, and asserted that they would not have purchased the vehicles or that they paid an inflated price for their vehicles.

Consistent with the *Clapper* decision, the court recently dismissed the plaintiffs' complaint (with leave to amend) for a lack of standing, finding that the plaintiffs did not allege that their or any other class members' cars have been hacked and therefore their alleged injuries are not certainly impending, but rather speculative and unproven *at this point*. Notably, the court emphasized the lack of any actual incidents of car hacking suffered by the class plaintiffs, or any other plaintiffs, outside of a controlled environment. The court suggested that it might arrive at a different conclusion on the issue of standing should a Connected Car actually be hacked, noting that "all of this is not to say that a future risk of harm can never satisfy injury in fact analysis" and that "a credible threat of harm is sufficient to constitute actual injury for standing purposes."

The court also rejected the plaintiffs' claims for economic loss, finding a lack of any demonstrable impact on the value of the vehicles such as declining values, recalls, or out-of-pocket expenses for replacing or discontinuing use of their vehicles. Finally, the court distinguished driver, performance, and location data from Social Security numbers or payment card numbers, finding that this type of data is not protected under California state privacy laws.

Plaintiffs assert similar claims in another class action pending in Illinois federal court, which also includes a claim against the vehicle "infotainment" manufacturer. Plaintiffs allege that the vehicle infotainment system is part of a design defect in the vehicle because it is not properly separated from the vehicle CAN system that connects to the vehicle engine control units and is susceptible to being hacked (via the 3G cellular network and radio connection). The vehicle computer system defendants argue that the plaintiffs' claims against them should be dismissed due to a lack of privity or any other actionable relationship between the plaintiffs and the vehicle infotainment manufacturer. The lack of any actual instances of cars being hacked could determine the outcome here, just as it did in the California litigation. Nonetheless, this case warrants following as it involves the potential liability of the component part manufacturers for data privacy and security vulnerabilities in Connected Cars.

Impact on Regulatory Framework

The evolving nature of the regulatory framework creates uncertainty for automakers, manufacturers, and technology companies that are attempting to innovate in this field. As the regulatory framework around Connected Cars evolves, it will be important for companies to keep apprised of new litigation and agency, industry, and legislative developments while maintaining flexibility in their products should new or stricter privacy and security standards be implemented or other regulators step into the fray.

As it stands, class action plaintiffs still face an uphill battle in bringing claims related to the data privacy and security of Connected Cars. Courts do not appear inclined to allow class plaintiffs to proceed on claims where no actual injury (hacking) has been manifested. Of course, if reports of actual incidents of car hacking begin to occur and there are actual instances of harm, the potential impact to businesses from the litigation and legislation that such instances might inspire could be significant.

Indeed, even the current legislation proposed by the Senate and House bills could create rigid compliance standards that could be costly, inefficient, and ineffective for protecting consumer privacy and securing vehicle safety as they are bypassed by hackers. The legislation could also subject companies that have made reasonable efforts to implement privacy and security standards to fines, and deter vehicle computer system security research. Importantly, onerous legislation could stifle innovation in the Connected Car arena by placing unnecessary limitations on the design and development of Connected Car computer systems.

For now, companies involved as stakeholders in developing privacy and data security standards for Connected Cars need to continue to remain aware of efforts by non-stakeholders to regulate this fast-moving technology. The privacy framework set forth in the Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services will likely be considered by regulators investigating these practices by automakers, manufacturers, and tech companies following a breach. The principles are largely consistent with the legislation proposed by Congress, but notably lack the guidance on security standards for Connected Cars to prevent hacking into Connected Car computer systems contained in the proposed legislation.

Companies also should continue to monitor guidance, enforcement activities, and investigations by the FTC and NHTSA. NHTSA is actively developing cybersecurity guidelines and best practices for securing automotive computer systems and reducing vulnerabilities. In addition, the FTC has expressly encouraged companies to build security into their products along with policies ensuring data minimization, notice, and choice. The use of guidelines and best practices by enforcement agencies, rather than calls for congressional action, suggests that agencies are content to allow the Connected Car industry to self-regulate at this time. Consequently, the more companies conform with this existing regulatory framework and show effectiveness in protecting consumer data from hackers, the less likely legislators are to push for specific privacy or cybersecurity legislation relating to Connected Cars. Further, companies that comply with the industry self-regulatory and agency guidance should be better positioned to defend against any claims in purported class actions that the company failed to follow reasonable privacy and security standards.

The Long View

The impact of the development of the regulatory framework governing Connected Cars on the development of IoT regulation as a whole cannot be underestimated. Many of the same privacy, data security, and physical safety concerns that arise with Connected Cars also arise with health devices, home automation systems, and smart energy grids. As a result, the industry response to the existing Connected Car regulatory framework, and the government's assessment of the efficacy of self-regulation on consumer protection, will likely determine whether this framework is applied in other IoT settings or replaced with more government regulation.

Legal Developments in Connected Car Arena Provide Glimpse of Privacy and Data Security Regulation in Internet of Things

By F. Paul Pittman*

February 2, 2016

*The author may be contacted at Paul.Pittman@whitecase.com

With the holiday season in the rear view, automobiles equipped with the newest technology connecting carmakers with their vehicles, vehicles with the world around them, and drivers with the consumer marketplace – Connected Cars – have moved from the lots to driveways. Automakers are remaking their fleets to offer unprecedented choice and convenience to drivers. However, as recent studies have shown, the connectivity inherent in Connected Cars, and the fast pace at which the industry is developing, raise privacy, data security, and physical safety concerns about the vulnerability of Connected Car computer systems. Lawmakers and regulators have begun to devote increased attention to this issue while plaintiffs' attorneys have been emboldened to haul automakers, manufacturers, and computer system developers into court. As one of the earliest entrants into and faster-growing components of the Internet of Things (IoT), Connected Cars represent a testing ground for the development of consumer privacy rights and security standards for the IoT. The approach by Congress and the courts to the governance of Connected Cars will likely guide the development of standards and practices across the IoT spectrum.

Internet of Things

Connected Cars are part of the growing and evolving Internet of Things. The IoT describes the ecosystem of everyday products and services that are equipped with "smart" technology that allows them to connect to other products or services to communicate and transfer information about users to retailers, manufacturers, and the like, typically via a wireless network. The IoT currently includes devices we use every day such as Fitbits, connected appliances, smartphones and smart TVs. As the industry grows, IoT devices will continue to permeate the objects we use on a daily basis.

Connected Cars in particular will compose the majority of the automotive fleet in the near future. The market for Connected Cars is projected to reach $54 billion in the next two years. It is estimated that by 2020 there will be 250 million Connected Cars on the road, and about 90 percent of new vehicles in Western Europe will be connected to the Internet. Connected Cars provide consumers with convenience and a personalized driving experience. Automakers and retailers gain access to consumers to provide improved services and to market

products. Onboard computers allow for navigation technologies and integration with mobile devices that complement and enhance the vehicle technology. They also allow for the collection of driver data and other driver information to enable companies to efficiently deploy customized services and experiences. Automakers are developing Connected Car technology that will allow drivers to shop through the car dashboard, based on their location and preferences determined through data collection.

Connected Car Privacy and Security Vulnerabilities

The connectivity necessary for providing the features offered by Connected Cars may pose privacy and security dangers and vulnerabilities. Connected Cars can contain more than 50 separate electronic control units (ECUs) connected through a controller area network (CAN) or other network. Those ECUs communicate with each other and the CAN through use of digital messages called CAN packets. If CAN packets are not authenticated or encrypted, they may be susceptible to remote hacking through the vehicles' wireless and phone components. This wireless technology may also enable unauthorized access to other systems and data collected by the vehicle, such as location data and potentially payment card data used for dashboard shopping.

There are also concerns about Connected Cars being subject to remote interference and operation. Security researchers' published findings have sparked increased industry, regulatory, and congressional interest in this area. One notable example involved a report that researchers were able to remotely access a car and change the car's air-conditioning settings, switch the volume and station on the radio, turn on the windshield wipers, and display a picture of the researchers on the digital dashboard screen from 10 miles away. The researchers also were able to disable the vehicle's engine and brakes, control the steering wheel, and track the car's GPS coordinates. The researchers claim that they could gain access to the vehicle from as far as 70 miles away.

Evolving Legal Landscape

Proposed Legislation

As manufacturers develop the vehicles and infrastructure that enable the use of Connected Cars, the legal landscape is struggling to keep up. Congress has proposed but has not enacted new legislation. On July 21, 2015, Senators Edward Markey (D-Mass.) and Richard Blumenthal (D-Conn.) proposed legislation (S. 1806) requiring the Department of Transportation's National Highway Traffic Safety Administration (NHTSA) to team with the Federal Trade Commission (FTC) to establish certain consumer data privacy and car computer network security rules to prevent hacking in all motor vehicles manufactured for sale in the U.S. ("SPY Car Act"). The SPY Car Act was based on a February 2015 report by Senator Markey, who had surveyed automakers about cybersecurity threats to safety and the collection and storage of driving data, including location, driving history, and user data. The report found that nearly all cars on the market have wireless technologies and identified several purported weaknesses in the security of connected features in cars.

The SPY Car Act would require collaboration between the NHTSA and the FTC to implement cybersecurity standards for vehicle system and driving data security, including

- hacking protection and mitigation;
- a "cyber dashboard" display label affixed to the vehicle that describes the vehicle's compliance with cybersecurity and privacy requirements under the SPY Car Act; and
- certain privacy standards including providing notice and choice regarding the use and collection of data, and limiting the use of driving data by manufacturers. Violators of the SPY Car Act cybersecurity standards would be penalized up to $5,000 per violation.

Violations of the privacy standards would be treated as unfair and deceptive acts or practices under Section 5 of the FTC Act.

In addition, in October 2015, Representatives Joe Wilson (R-S.C.) and Ted Lieu (D-Calif.) suggested legislation titled Examining Ways to Improve Vehicle and Roadway Safety: Vehicle Data Privacy that would require auto manufacturers to:

- develop and implement a privacy policy regarding the collection, sharing, and use of driver and vehicle data;
- file their privacy policies with the Secretary of Transportation;
- retain data only for legitimate business purposes; and
- implement reasonable security measures to prevent hacking. The proposed legislation would impose on auto manufacturers penalties of up to $1 million for failing to file a privacy policy or comply with an express privacy policy and fines of up to $100,000 for failing to prevent hacking.

The proposed legislation would also require the NHTSA to create an Automotive Cybersecurity Advisory Council to develop cybersecurity best practices for vehicle manufacturers.

Notably, the proposed legislation contains a safe harbor against FTC enforcement under Section 5 of the FTC Act for companies that file a privacy policy complying with these requirements. Unsurprisingly, the FTC has expressed disapproval of this provision, which could provide immunity to an auto manufacturer that does not follow its privacy policy and prohibit the FTC from enforcement actions against auto manufacturers for privacy-related misrepresentations on their websites, whether accessed through the vehicle or otherwise.

Self-Regulation

The automotive industry and even the FTC have cautioned that IoT-specific legislation may stifle IoT innovation and penalize companies that attempt to implement reasonable privacy and security measures. Many lawmakers have little understanding of the IoT and are not yet equipped to address the issues it presents.

Notably, and despite the pending proposed SPY Car Act, the Senate passed a resolution on March 24, 2015, that recognizes the importance of the development of the IoT and resolves that public and private entities should guide the strategy for advancing the technology. The resolution calls for Congress and the industry to collaborate to advance a national Internet of Things strategy that does not result in overregulation that stifles and prevents innovation and growth.

The automotive industry has also taken steps toward self-regulation. In November 2014, the Alliance of Automobile Manufacturers, Inc., and the Association of Global Automakers, Inc., published the Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services. These principles relate to the collection, use, and sharing of personal and vehicle information associated with vehicle technologies that collect, generate, record, and store this information. The principles call for automakers and manufacturers to ensure the following by 2017:

- provide consumers with clear notice and choice in the use and collection of personal information;
- use personal information in a way that is consistent with the context in which it was collected;
- collect information only as legitimately needed, and retain it for only as long as necessary;
- implement reasonable data security measures;
- maintain the accuracy of the data, and provide access to users; and
- remain accountable to consumers for adherence to these principles.

The Alliance of Automobile Manufacturers, Inc., and the Association of Global Automakers, Inc., have also formed an Information Sharing and Analysis Center (ISAC) to share intelligence about vehicle cybersecurity threats and designed a framework to further the development of automotive cybersecurity best practices on how to safeguard against and respond to threats.

Enforcement

Whether the regulatory framework surrounding Connected Cars emanates from legislation or self-regulation, several agencies are poised to take the lead in enforcement activities in the area. In fact, the SPY Car Act requires collaboration between the FTC and the NHTSA in developing privacy and security standards for Connected Cars. The FTC has traditionally been the lead regulator of consumer privacy and data security standards by using its authority under Section 5 of the FTC Act to contend that a lack of reasonable security measures or other missteps amount to unfair or deceptive acts or practices. The FTC has indicated an intent to play a similar role with regard to Connected Cars as evidenced by the guidance IoT document it issued titled Internet of Things – Security and Privacy in a Connected World. This guidance document encourages companies operating in the IoT to implement "security by design" into their products, along with providing consumers notice and choice with regard to collection and use of the personal information, and ensuring that companies' data collection and use practices are transparent and minimize data collection, among other suggested best practices.

NHTSA is a relatively new entrant into the data privacy and security enforcement arena, but it will be tasked with ensuring that automakers and manufacturers implement security standards sufficient to protect Connected Car computer systems from being accessed and physically controlled. NHTSA has published guidance on automotive cybersecurity, including application of the National Institute of Standards and Technology (NIST) Risk Management framework in the automotive cybersecurity context. And NHTSA recently completed an investigation of an auto manufacturer and its computer system vendor related to vehicle cybersecurity, which is particularly important since some technology company vendors supply these same systems to other car manufacturers. Automakers appear to be receptive to NHTSA's approach as they recently announced a data sharing safety agreement that reaffirms the commitment of NHTSA and automakers to collaborate on the development of cybersecurity best practice, and the continued sharing of information on cybersecurity threats and countermeasures to repel potential hackers. As Connected Car technology grows to encompass more products and services, the Federal Communications Commission (FCC) may also emerge as an enforcement player under its expanded enforcement authority over "telecommunications service" providers. Internet service providers that offer the wireless Internet services that fuel Connected Car connectivity could face increased scrutiny by the FCC, and potential fines, over the adequacy of their privacy practices and security standards for the collection of consumer personal information crossing their wireless networks.

Litigation

Class actions alleging claims based on privacy and security issues related to Connected Cars have already been filed. In an action filed in California federal court, the plaintiffs sought to certify a class of car owners who allege that the defendant car manufacturers created and concealed data privacy and vehicle security vulnerabilities through the continued use of the CAN system. The plaintiffs alleged that the CAN system is susceptible to being hacked, which could allow for the collection of data stored on the CAN system and for the control of certain vehicle functions such as steering, braking, and acceleration. The plaintiffs asserted claims for express and implied breach of warranty, fraud, false advertising, and violations of consumer protection laws. The plaintiffs sought injunctive relief, updates to the CAN system to secure and protect vehicles and data, and recovery of economic losses associated with the loss of their vehicles' value.

The defendant car manufacturers moved to dismiss the action, arguing that the plaintiffs did not suffer any "injury in fact" because their cars have not been hacked or taken control of, nor had their data been breached. The defendants relied primarily on *Clapper v. Amnesty Int'l,* where the Supreme Court held that to establish standing, a plaintiff must allege more than a speculative injury, but rather the injury alleged must be "concrete and particularized" and "actual or imminent." The defendants also asserted that the plaintiffs lacked standing to bring an invasion of privacy claim because the plaintiffs did not have a reasonable expectation in the privacy of the personal data collected by the Connected Car and that the type of data collected did not cause a "serious invasion of privacy." The plaintiffs claimed that they had been injured by the defendant car manufacturers' alleged misrepresentations about the alleged privacy and security defects, and asserted that they would not have purchased the vehicles or that they paid an inflated price for their vehicles.

Consistent with the *Clapper* decision, the court recently dismissed the plaintiffs' complaint (with leave to amend) for a lack of standing, finding that the plaintiffs did not allege that their or any other class members' cars have been hacked and therefore their alleged injuries are not certainly impending, but rather speculative and unproven *at this point*. Notably, the court emphasized the lack of any actual incidents of car hacking suffered by the class plaintiffs, or any other plaintiffs, outside of a controlled environment. The court suggested that it might arrive at a different conclusion on the issue of standing should a Connected Car actually be hacked, noting that "all of this is not to say that a future risk of harm can never satisfy injury in fact analysis" and that "a credible threat of harm is sufficient to constitute actual injury for standing purposes."

The court also rejected the plaintiffs' claims for economic loss, finding a lack of any demonstrable impact on the value of the vehicles such as declining values, recalls, or out-of-pocket expenses for replacing or discontinuing use of their vehicles. Finally, the court distinguished driver, performance, and location data from Social Security numbers or payment card numbers, finding that this type of data is not protected under California state privacy laws.

Plaintiffs assert similar claims in another class action pending in Illinois federal court, which also includes a claim against the vehicle "infotainment" manufacturer. Plaintiffs allege that the vehicle infotainment system is part of a design defect in the vehicle because it is not properly separated from the vehicle CAN system that connects to the vehicle engine control units and is susceptible to being hacked (via the 3G cellular network and radio connection). The vehicle computer system defendants argue that the plaintiffs' claims against them should be dismissed due to a lack of privity or any other actionable relationship between the plaintiffs and the vehicle infotainment manufacturer. The lack of any actual instances of cars being hacked could determine the outcome here, just as it did in the California litigation. Nonetheless, this case warrants following as it involves the potential liability of the component part manufacturers for data privacy and security vulnerabilities in Connected Cars.

Impact on Regulatory Framework

The evolving nature of the regulatory framework creates uncertainty for automakers, manufacturers, and technology companies that are attempting to innovate in this field. As the regulatory framework around Connected Cars evolves, it will be important for companies to keep apprised of new litigation and agency, industry, and legislative developments while maintaining flexibility in their products should new or stricter privacy and security standards be implemented or other regulators step into the fray.

As it stands, class action plaintiffs still face an uphill battle in bringing claims related to the data privacy and security of Connected Cars. Courts do not appear inclined to allow class plaintiffs to proceed on claims where no actual injury (hacking) has been manifested. Of course, if reports of actual incidents of car hacking begin to occur and there are actual instances of harm, the potential impact to businesses from the litigation and legislation that such instances might inspire could be significant.

Indeed, even the current legislation proposed by the Senate and House bills could create rigid compliance standards that could be costly, inefficient, and ineffective for protecting consumer privacy and securing vehicle safety as they are bypassed by hackers. The legislation could also subject companies that have made reasonable efforts to implement privacy and security standards to fines, and deter vehicle computer system security research. Importantly, onerous legislation could stifle innovation in the Connected Car arena by placing unnecessary limitations on the design and development of Connected Car computer systems.

For now, companies involved as stakeholders in developing privacy and data security standards for Connected Cars need to continue to remain aware of efforts by non-stakeholders to regulate this fast-moving technology. The privacy framework set forth in the Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services will likely be considered by regulators investigating these practices by automakers, manufacturers, and tech companies following a breach. The principles are largely consistent with the legislation proposed by Congress, but notably lack the guidance on security standards for Connected Cars to prevent hacking into Connected Car computer systems contained in the proposed legislation.

Companies also should continue to monitor guidance, enforcement activities, and investigations by the FTC and NHTSA. NHTSA is actively developing cybersecurity guidelines and best practices for securing automotive computer systems and reducing vulnerabilities. In addition, the FTC has expressly encouraged companies to build security into their products along with policies ensuring data minimization, notice, and choice. The use of guidelines and best practices by enforcement agencies, rather than calls for congressional action, suggests that agencies are content to allow the Connected Car industry to self-regulate at this time. Consequently, the more companies conform with this existing regulatory framework and show effectiveness in protecting consumer data from hackers, the less likely legislators are to push for specific privacy or cybersecurity legislation relating to Connected Cars. Further, companies that comply with the industry self-regulatory and agency guidance should be better positioned to defend against any claims in purported class actions that the company failed to follow reasonable privacy and security standards.

The Long View

The impact of the development of the regulatory framework governing Connected Cars on the development of IoT regulation as a whole cannot be underestimated. Many of the same privacy, data security, and physical safety concerns that arise with Connected Cars also arise with health devices, home automation systems, and smart energy grids. As a result, the industry response to the existing Connected Car regulatory framework, and the government's assessment of the efficacy of self-regulation on consumer protection, will likely determine whether this framework is applied in other IoT settings or replaced with more government regulation.