Spring Meeting 2019

Intellectual Property Law Section

April 5, 2019

Davis Polk & Wardwell LLP

450 Lexington Ave, New York, NY 10017

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/IPSSpring19Materials/

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 Spring Meeting 2019**
Date: April 5, 2019 Location: New York, NY

Evaluation: https://nysba.co1.qualtrics.com/jfe/form/SV_6x2ovNsrGwiweyN
This evaluation survey link will be emailed to registrants following the program.

Total Credits: **8.0 New York CLE credit hours**

Credit Category:
4.0 Areas of Professional Practice
2.0 Ethics and Professionalism
2.0 Law Practice Management

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

SPRING MEETING 2019

EMERGING TRENDS IN INTELLECTUAL PROPERTY AND ETHICAL CONSIDERATIONS FOR LAWYERS:

LAWYERING IN THE AGE OF BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

http://www.nysba.org/IPSSpring19/

Presented by the NYSBA Intellectual Property Section

April 5, 2019

Davis Polk & Wardwell LLP
450 Lexington Avenue | New York, NY 10017

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

PROGRAM CHAIRS
Daniel F. Forester, Esq. | Davis Polk & Wardwell LLP | New York
Leonie Huang, Esq. | Holland & Knight LLP | New York

Program Description

The legal profession is buzzing with talk of transformative innovations that are reshaping business and legal practices. This program will provide an in-depth look at blockchain and advances in artificial intelligence to assist legal practitioners navigate and shape the changing landscape.

Appropriate for both new associates and seasoned practitioners, this program will provide an overview of fast-growing emerging technologies in the blockchain and artificial intelligence space, related key legal updates pertinent to core IP practices, and practical advice for advising clients on these new technologies. The ethics component offers 2 CLE Ethics Credits, with a panel focused on ethical considerations related to information gathering and evolving technologies.

7:50-8:25 a.m.	Registration and Continental Breakfast
8:25-8:30 a.m.	Welcoming Remarks
8:30-9:45 a.m.	**Blockchain Basics. What it is, how it works, and why it matters.** *This panel will explore the basics of blockchain technology, and provide practical background on what it is, how it works, and the various types of blockchain already in use and still emerging. The panel will also discuss what industries are currently adopting blockchain, how it is transforming those industries, business processes, current and emerging regulation, and what is yet to come.*

Understanding the basics will not only assist attorneys to competently evaluate the legal concerns facing clients, but will also help attorneys to keep abreast of the benefits and risks associated with blockchain technologies as they affect services provided by legal professionals. (1.0 CLE Credits - Areas of Professional Practice and 0.5 CLE credits - Law Practice Management)

Moderator: **Preston Byrne**, Partner, Byrne & Storm, P.C.
Speakers: **Jakki Kerubo**, Founder, Novum Communications Consulting
Greg Piccolo, Lead Engineer, Jigsaw XYZ

9:45-10:00 a.m. Morning Break

10:00-11:15 a.m. **What IP Practitioners Should Know about Blockchain.**

This panel will consider the key intellectual property issues developing around blockchain, how blockchain intersects with current forms of IP protection, and provide practical advice for counseling clients on protecting their IP and legal solutions for their business. The panel will also inform IP practitioners on the emerging regulatory considerations for digital assets, virtual currency, and risks and benefits of innovative capital-raising strategies. (1.5 CLE credits - Areas of Professional Practice)

Moderator: **Preston Byrne**, Partner, Byrne & Storm, P.C.
Speakers: **Joshua Krumholz**, Partner, Holland & Knight LLP
Jennifer Connors, Partner, Holland & Knight LLP

11:15-12:05 p.m. **Ethical Considerations in Information Gathering and Evolving Technologies.**

Investigations are an essential element of most litigation matters. Practitioners working in IP and brand protection matters often need due diligence information about their clients' litigation adversaries, the owner of a trademark, or the target of a counterfeiting investigation, for example. It's vital to understand the ethical limitations for conducting an investigation, including application of ethical obligations in situations related to determining what information is relevant and where an attorney may ethically obtain that information.

This presentation will address understanding what an attorney can and cannot have investigators do, the difference between ethical violations and criminal violations, the types of due diligence information that is available on individuals and corporations without violating an attorney's ethical obligations, and practical ethical considerations when conducting field investigations (including issues arising related to witness statements, surveillance and location investigations), distinctions between an investigation in the United State versus one conducted in other countries and how that could change the relevant ethical considerations, and learning about how technology is affecting investigations and raising new ethical issues.
(1 CLE credit - Ethics and Professionalism)

Speaker: **William Belmont**, The Belmont Group, LLC

12:05-1:00 p.m. Lunch

1:00-1:50 p.m. **Ethical Considerations in Information Gathering and Evolving Technologies.**

This presentation continues with additional discussion on the ethical considerations and professional conduct rules related to attorney gathering of information, international aspects of information gathering and use, the use of investigators, and information-gathering issues related to use of social media, mobile apps and mobile devices, cloud computing and cloud services, remote access, data monetization and privacy issues, as well as protecting against leaks of confidential and privileged information. (1 CLE credit - Ethics and Professionalism)

Speaker: **Pery D. Krinsky**, Krinsky PLLC

1:50-2:00 p.m. Afternoon Break

2:00-4:30 p.m. **Artificial Intelligence and the Law – A primer for lawyers. Will we all become obsolete?**

Machine Learning. Natural Language Processing. Artificial Intelligence. These buzzwords and concepts are already in – or are coming soon – to a business, and a law firm near you. This panel will explore the nuts and bolts of AI and how it is poised to change the legal landscape. The panel will take participants along for a deep-dive into the technical, legal, and social impacts of AI. In particular, the panelists will investigate how the legal profession will adapt to the new AI-based tools at its disposal.

Understanding the benefits and risks of AI technology will be important for attorneys to consider in evaluating technologies used in providing legal services and in competently identifying legal considerations and risks facing clients. (1.5 CLE credits - Law Practice Management)

AI can serve as a technological marvel, but its use brings with it a host of new legal questions, including those with respect to inventorship, liability and regulatory applicability—as just some examples. (1.5 CLE credits - Areas of Professional Practice)

Moderators: **Rory Radding**, Partner, Locke Lord LLP
Alexander Puutio, Administrative Officer, United Nations

Speakers: **Diane Holt**, Team Lead – Transactions, Bloomberg Law – *Introduction to AI*
Rory Radding, Partner, Locke Lord LLP – *AI and Intellectual Property*
Jonathan Askin, Professor, Brooklyn Law School – *AI, IP and Legal Tech*
Matthew D'Amore, Associate Dean, Cornell Tech – *AI in Law Practice and Legal Education*
Ned Gannon, President, eBrevia – *Application of AI in the Legal Profession*
Alexander Puutio, Administrative Officer, United Nations – *AI in the Global Context, a Summary*

4:30-6:00 p.m. **Networking Reception - Sponsored by:** CompuMark
Trademark Research and Protection

NEW YORK STATE BAR ASSOCIATION
INTELLECTUAL PROPERTY LAW SECTION

Spring Meeting 2019

Emerging Trends in Intellectual Property and Ethical Considerations for Lawyers

Thank you to our Networking Reception Sponsor:

CompuMark
Trademark Research and Protection

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

Blockchain Basics.
What It Is, How It Works, and Why it Matters.

Preston Byrne (Moderator)
Partner, Byrne & Storm, P.C.

Jakki Kerubo
Founder, Novum Communications Consulting

Greg Piccolo
Lead Engineer, Jigsaw XYZ

BLOCKCHAIN BASICS FOR THE LEGAL PRACTITIONER

By: Preston J. Byrne, Partner, Byrne & Storm, P.C.

1. BLOCKCHAIN 101

1.1. Bitcoin (proposal published 2008, paper released 2009) was the first true "blockchain" system. A blockchain is a *database.* Furthermore, it is a *peer-to-peer*, *distributed* database.

1.2. A blockchain database differs from other types of distributed databases because it has certain properties which make it *fault-tolerant*, i.e., even if one computer operating a piece of the blockchain, known as a *node*, fail, the rest of the network can continue to operate.

1.3. Blockchain fault-tolerance is also sometimes described as being *Byzantine* fault tolerant, a term of art which means that a blockchain should run even if the failure of a particular component, or a significant number of components, is caused not by an innocent failure but rather by a malicious attacker gaining control of a large number of nodes.

1.4. Blockchain nodes communicate with one another through peer-to-peer networking protocols over TCP-IP, much like the rest of the Internet. However, with blockchains, nodes communicate with each other directly (e.g. as BitTorrent does with the BitTorrent Mainline DHT[1]) rather than through a central server found at a particular address (e.g. https://facebook.com). These communications may or may not be encrypted.

1.5. Blockchain systems are, generally speaking, designed to communicate *economically significant transactional data.* Blockchains use cryptography to verify whether transactional communications are *valid.* If a blockchain node receives a valid communication, it will propagate that valid communication to other network nodes, with the consequence that the copy of the valid communication should eventually be written to the local copy of the receiver's blockchain and every other copy of the chain.

1.6. If a blockchain receives an invalid communication, the data will be rejected by an honest node and that node will not propagate the transaction to other nodes on the network. receiver and will not appear on the blockchain. Due to this, much like in commercial transactions transactional lawyers work with on a daily basis, a transaction on a blockchain "either completes or doesn't occur at all, and can't be left in an intermediate state."[2]

1.7. Valid transactions are batched together by individual nodes as they are received. Both the procedure, and end-state, whereby every node on a blockchain comes to an agreement that all of the transactions recorded on a blockchain are valid, are each referred to in the industry by the term "consensus." Consensus ensures that every blockchain node sees the same data as every other blockchain node.

1.8. This batching procedure, and resultant end-state, whereby every node on a blockchain arrives at an agreement that all of the transactions recorded on a blockchain are valid, are each referred to in the industry by the term "consensus." Consensus ensures that every blockchain node sees the same data as every other blockchain node.

[1] "DHT" means "Distributed Hash Table."
[2] Buchman, Ethan. *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains,* p. 5. https://atrium.lib.uoguelph.ca/xmlui/handle/10214/9769

1.9. A node with permission to validate transactions, sometimes known as a *validator node*, has the power to decide that a number of transactions it has seen is valid.

1.10. In most blockchain systems, a validator node will batch transactions in a data structure which is known as a *block* and propose the inclusion of the block of transactions to the other validator nodes. Put another way, it asks the other validator nodes for their approval and consent to the block's inclusion in the blockchain database.

1.11. If a requisite majority of the other validator nodes agree that the block is also valid, then that block will be published to or adopted by the network, sometimes together with separate cryptographic proof of the validator nodes' collective consent. As part of this process, the validator nodes will also embed cryptographic proofs in each new block which are linked to certain cryptographic proofs in the previous block. This ensures that any tampering with any data in any prior block in the chain of blocks, or *blockchain*, will be immediately apparent to an observer looking at the present state of the data.

1.12. Once a block is agreed and published, it is appended to the end of the blockchain and the process begins anew, with new transactions being received by validator nodes and, in due time, being proposed to the network to form new blocks. How frequently this procedure repeats itself is dependent on the underlying architecture used by the blockchain in question. Currently there is a broad range, with systems like Bitcoin publishing new blocks that the network agrees on, i.e. *confirm* a block, on average every six minutes, and other systems, e.g. Tendermint, being able to confirm blocks once per second.

2. CRYPTOCURRENCIES: THE FIRST BLOCKCHAIN APPLICATION

2.1. ***Examples of virtual currencies***

2.1.1. **Bitcoin.** The first cryptocurrency, based on proof of work consensus.

2.1.2. **Ripple or Stellar.** Other early cryptocurrencies, based on proof of stake consensus.

2.1.3. **Dogecoin**. A so-called "altcoin," one of thousands of altcoins, with few technical differences between itself and Bitcoin. Altcoins' focus can be entirely arbitrary; in Dogecoin's case, the coin is themed around a cute Shiba Inu dog.

2.1.4. **Ethereum**. An altcoin that allows coin holders to upload scripts, known as "smart contracts," on the blockchain. "Smart contracts" are not smart and are not contracts, but allow users of cryptocurrency systems to model financial contracts (such as escrow, collateralized lending, or prediction markets) in blockchain code which settle entirely on-chain. Systems like Tezos or Eos are also smart contract systems.

2.2. ***Cryptocurrencies are not all the same***

2.2.1. Most major cryptocurrencies use the same elliptic curve cryptography for signing transactions, but do not encrypt transactions or data. Exceptions to the rule include ZCash and Monero, which do encrypt transactions and data.

2.2.2. Most major cryptocurrency protocols are licensed for free public use under open-source licenses. MIT, Apache 2.0, and GPL 3.0 are popular licensing schemes.

2.2.3. Cryptocurrencies differ from each other mostly on (a) how they achieve consensus, (b) what type of data they allow their users to communicate, and (c) performance characteristics.

2.2.4. **Proof of work** cryptocurrencies use a competitive game that requires the consumption of vast quantities of electricity to determine block-by-block consensus through a process known as **mining.** Bitcoin and Ethereum are examples of proof of work cryptocurrencies.

2.2.5. **Proof of stake** cryptocurrencies allow holders of existing quantities of the native cryptocurrency to vote on which transaction should be included in the next block through a process known as **staking.** Tendermint and NXT are examples of proof of stake cryptocurrencies. There are variations on proof of stake, such as "delegated proof of stake," utilized by cryptocurrencies such as Eos.

2.2.6. **Developers are constantly looking for new and better ways to achieve consensus on blockchain networks,** such as the "proof of space and time" method being used by Chia (founded by Bram Cohen, founder of BitTorrent).

2.2.7. **Transaction speeds vary widely.** Because cryptocurrencies are stateful systems, i.e. blockchain networks store all data that has ever been sent to them, developers of these systems need to make tradeoffs between performance and scalability. Where a system is designed to handle high transaction throughputs and data-heavy transactions, such as Ethereum (14 transactions per second/TPS plus smart contract code), the blockchain will swell in size, or *bloat*, making it difficult for ordinary users to run blockchain nodes.

2.2.8. **"How decentralized is it?"** …is never an easy question to answer. When this term, "decentralization," comes up, it can mean one of a number of things, including (a) how large and distributed the network of nodes is for a given network, (b) the chosen consensus mechanism being used by a given network, (c) the distribution model for coins issued on/by a given network, or (d) a range of other factors the market latches onto from time to time. The term lacks a concrete legal or technical definition, although senior officials of the U.S. Securities and Exchange Commission have tried to use the concept to determine the applicability of U.S. securities laws to cryptocurrency systems.[3]

2.3. ***Major legal issues arising from the cryptocurrency context***

2.3.1. **Anti money laundering/money transmitter licensing is** central to any cryptocurrency business.

2.3.1.1. Small-time Bitcoin exchangers have been charged with operating unlicensed money transmission businesses under 18 U.S.C. § 1960.

[3] Hinman, William. *Digital Asset Transactions: When Howey met Gary (Plastic.)* 14 June 2018, *https://www.sec.gov/news/speech/speech-hinman-061418*

2.3.1.2. **Required reading**: FinCEN 2013 Guidance defining "users," "administrators" and "exchangers"[4] of cryptocurrency systems

2.3.1.3. **Note "Layer 2" solutions** like Lightning Network do not eliminate money transmission concerns and require a standalone analysis depending on the design of the proposed application.

2.3.2. **Securities regulation:** a prevailing view among venture capitalists and others in the 2015-17 period was that securities regulation would be swept aside like municipal taxi regulations were swept aside by Uber. This view proved incorrect; practitioners should assume that, at point of issuance, all tokens are potentially securities and that if issued by companies should either be registered or benefit from an exemption to the registration requirement.

2.3.3. **Required reading:**

2.3.3.1. DAO Report of Investigation (SEC)[5]

2.3.3.2. Paragon/AirFox SEC Orders (non-registration of securities by issuer)[6]

2.3.3.3. EtherDelta SEC Order (non-registration of securities exchange)[7]

2.3.3.4. Crypto Asset Management, LP SEC Order (non-registration as investment adviser)[8]

2.3.3.5. U.S. v. Ignatov et al. indictments[9]

2.3.4. **New York Virtual Currency Business License ("Bitlicense")**

Required for, per 23 NYCRR 200.3(a):

- Receiving cryptocurrency for transmission *unless* for nonfinancial purpose and for a nominal amount
- Storing, holding, maintaining custody of cryptocurrency
- Buying and selling cryptocurrency as a customer business
- Performing exchange services as a customer business
- Controlling, administering or issuing cryptocurrency.

3. ENTERPRISE BLOCKCHAINS

3.1. ***What is an enterprise blockchain?***

3.1.1. An enterprise blockchain is a blockchain database that is not used in a "decentralized" manner.

[4] https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf
[5] https://www.sec.gov/litigation/investreport/34-81207.pdf
[6] https://www.sec.gov/litigation/admin/2018/33-10574.pdf
[7] https://www.sec.gov/litigation/admin/2018/34-84553.pdf
[8] https://www.sec.gov/litigation/admin/2018/33-10544.pdf
[9] https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-charges-against-leaders-onecoin-multibillion-dollar

3.1.2. Generally this means that *validator nodes* are identified in advance and controlled by known persons against whom legal recourse can be sought.

3.1.3. Possible range of applications as broad as software itself, generally focused on transaction and event control:

3.1.3.1. Payments and remittances (Ripple, R3)

3.1.3.2. Securities lifecycle automation (R3 Corda, JP Morgan's Quorum)

3.1.3.3. Hardware security and device authentication[10]

3.1.3.4. Supply chain automation and verification (IBM/Hyperledger Fabric frequently encountered)

3.1.3.5. Stock exchange infrastructure (Digital Asset Holdings, R3 Corda)

3.2. *What characteristics distinguish enterprise chains from cryptocurrencies?*

3.2.1. Cryptocurrencies express data mainly in the form as cryptocurrency token balances; enterprise blockchains do not need tokens to operate, and can therefore use more expressive smart contract scripts to describe and manage economically relevant events.

3.2.2. Validator/consensus arrangements usually follow what is required by the contractual terms of the transaction. So, e.g., a security might have consensus dictated by the note trustee working in concert with a platform provider.

3.2.3. Lawyers can be useful here in providing critical input to software design. Startup entrepreneurs often require a critical eye to ensure that their on-chain proposals and designs accurately reflect the commercial realities of the transactions they're trying to automate.

3.3. *Popular implementations*

3.3.1. R3 Interbank Consortium

3.3.1.1. Corda

3.3.2. The Hyperledger Consortium (under the auspices of the Linux Foundation)

3.3.2.1. Hyperledger Fabric (IBM blockchain protocol)

3.3.2.2. Hyperledger Sawtooth (Intel blockchain protocol)

3.3.2.3. Hyperledger Burrow (Monax blockchain protocol, Hyperledger's Ethereum Virtual Machine)

[10] See e.g. https://medium.com/blockchain-blog/blockchain-based-authentication-of-devices-and-people-c7efcfcf0b32
or
https://csrc.nist.gov/CSRC/media/Presentations/Leveraging-Blockchain-based-Protocols-in-IoT-Syste/images-media/1_iot_stavrous.pdf

3.3.2.4. Hyperledger Iroha (Soramitsu blockchain policy)

3.3.3. Ripple Labs

3.3.3.1. Ripple XRP (quasi-cryptocurrency) and Interledger (permissioned blockchain)

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

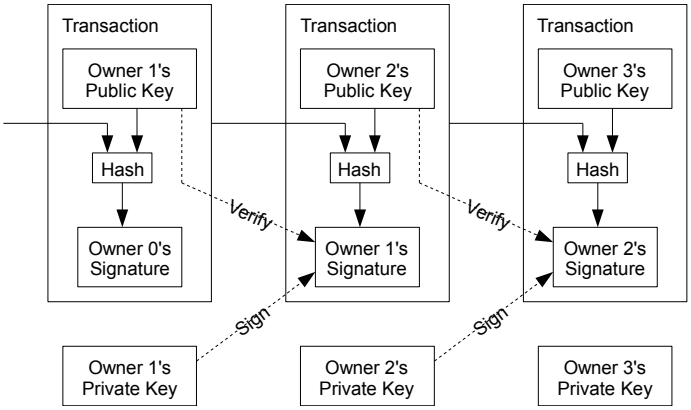
1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

2. Transactions

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.

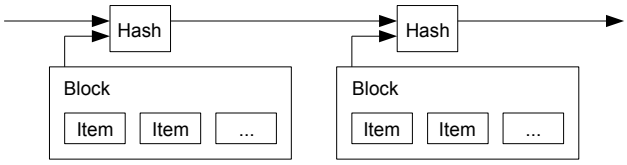


The problem of course is the payee can't verify that one of the owners did not double-spend the coin. A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending. After each transaction, the coin must be returned to the mint to issue a new coin, and only coins issued directly from the mint are trusted not to be double-spent. The problem with this solution is that the fate of the entire money system depends on the company running the mint, with every transaction having to go through them, just like a bank.

We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced [1], and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

3. Timestamp Server

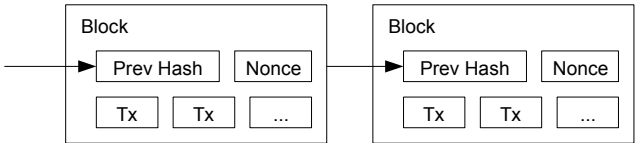
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post [2-5]. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system similar to Adam Back's Hashcash [6], rather than newspaper or Usenet posts. The proof-of-work involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.

For our timestamp network, we implement the proof-of-work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.



The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes. We will show later that the probability of a slower attacker catching up diminishes exponentially as subsequent blocks are added.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

5. Network

The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-work is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

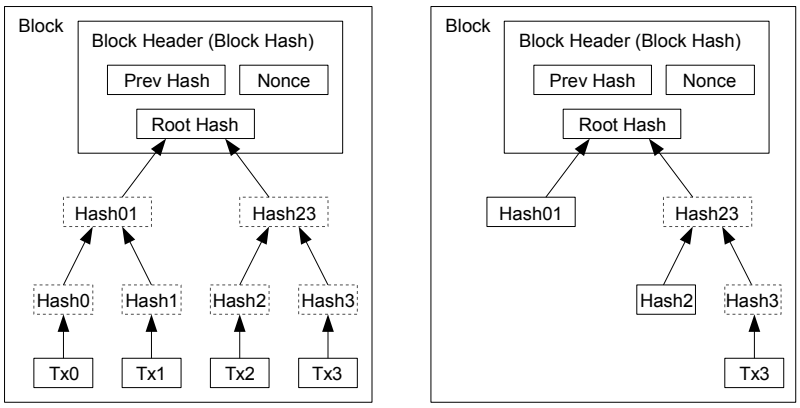
By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7. Reclaiming Disk Space

Once the latest transaction in a coin is buried under enough blocks, the spent transactions before it can be discarded to save disk space. To facilitate this without breaking the block's hash, transactions are hashed in a Merkle Tree [7][2][5], with only the root included in the block's hash. Old blocks can then be compacted by stubbing off branches of the tree. The interior hashes do not need to be stored.



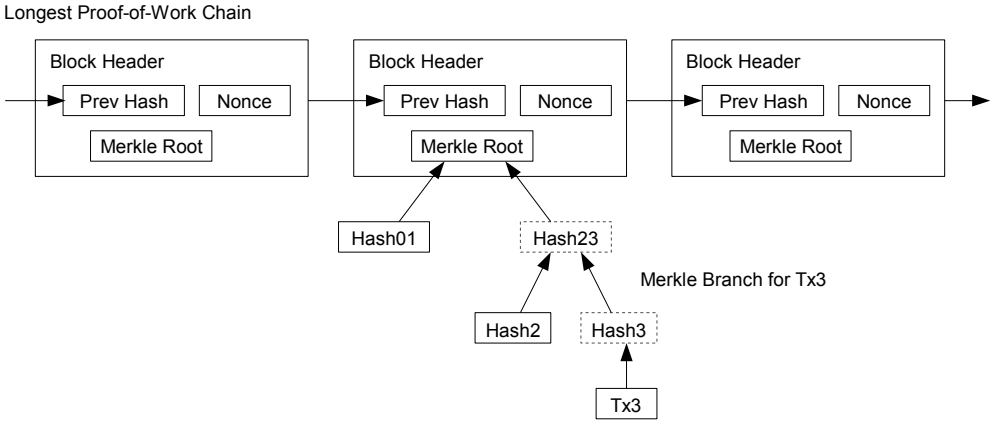
Transactions Hashed in a Merkle Tree

After Pruning Tx0-2 from the Block

A block header with no transactions would be about 80 bytes. If we suppose blocks are generated every 10 minutes, 80 bytes * 6 * 24 * 365 = 4.2MB per year. With computer systems typically selling with 2GB of RAM as of 2008, and Moore's Law predicting current growth of 1.2GB per year, storage should not be a problem even if the block headers must be kept in memory.

8. Simplified Payment Verification

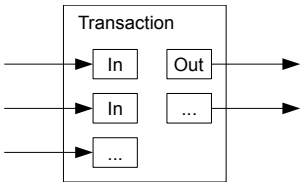
It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.



As such, the verification is reliable as long as honest nodes control the network, but is more vulnerable if the network is overpowered by an attacker. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transactions for as long as the attacker can continue to overpower the network. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency. Businesses that receive frequent payments will probably still want to run their own nodes for more independent security and quicker verification.

9. Combining and Splitting Value

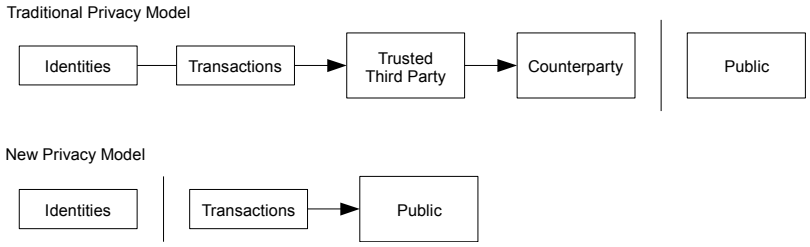
Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



It should be noted that fan-out, where a transaction depends on several transactions, and those transactions depend on many more, is not a problem here. There is never the need to extract a complete standalone copy of a transaction's history.

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

11. Calculations

We consider the scenario of an attacker trying to generate an alternate chain faster than the honest chain. Even if this is accomplished, it does not throw the system open to arbitrary changes, such as creating value out of thin air or taking money that never belonged to the attacker. Nodes are not going to accept an invalid transaction as payment, and honest nodes will never accept a block containing them. An attacker can only try to change one of his own transactions to take back money he recently spent.

The race between the honest chain and an attacker chain can be characterized as a Binomial Random Walk. The success event is the honest chain being extended by one block, increasing its lead by +1, and the failure event is the attacker's chain being extended by one block, reducing the gap by -1.

The probability of an attacker catching up from a given deficit is analogous to a Gambler's Ruin problem. Suppose a gambler with unlimited credit starts at a deficit and plays potentially an infinite number of trials to try to reach breakeven. We can calculate the probability he ever reaches breakeven, or that an attacker ever catches up with the honest chain, as follows [8]:

p = probability an honest node finds the next block
q = probability the attacker finds the next block
q_z = probability the attacker will ever catch up from z blocks behind

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Given our assumption that $p > q$, the probability drops exponentially as the number of blocks the attacker has to catch up with increases. With the odds against him, if he doesn't make a lucky lunge forward early on, his chances become vanishingly small as he falls further behind.

We now consider how long the recipient of a new transaction needs to wait before being sufficiently certain the sender can't change the transaction. We assume the sender is an attacker who wants to make the recipient believe he paid him for a while, then switch it to pay back to himself after some time has passed. The receiver will be alerted when that happens, but the sender hopes it will be too late.

The receiver generates a new key pair and gives the public key to the sender shortly before signing. This prevents the sender from preparing a chain of blocks ahead of time by working on it continuously until he is lucky enough to get far enough ahead, then executing the transaction at that moment. Once the transaction is sent, the dishonest sender starts working in secret on a parallel chain containing an alternate version of his transaction.

The recipient waits until the transaction has been added to a block and z blocks have been linked after it. He doesn't know the exact amount of progress the attacker has made, but assuming the honest blocks took the average expected time per block, the attacker's potential progress will be a Poisson distribution with expected value:

$$\lambda = z\frac{q}{p}$$

To get the probability the attacker could still catch up now, we multiply the Poisson density for each amount of progress he could have made by the probability he could catch up from that point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Rearranging to avoid summing the infinite tail of the distribution...

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

Converting to C code...

```
#include <math.h>
double AttackerSuccessProbability(double q, int z)
{
    double p = 1.0 - q;
    double lambda = z * (q / p);
    double sum = 1.0;
    int i, k;
    for (k = 0; k <= z; k++)
    {
        double poisson = exp(-lambda);
        for (i = 1; i <= k; i++)
            poisson *= lambda / i;
        sum -= poisson * (1 - pow(q / p, z - k));
    }
    return sum;
}
```

Running some results, we can see the probability drop off exponentially with z.

```
q=0.1
z=0     P=1.0000000
z=1     P=0.2045873
z=2     P=0.0509779
z=3     P=0.0131722
z=4     P=0.0034552
z=5     P=0.0009137
z=6     P=0.0002428
z=7     P=0.0000647
z=8     P=0.0000173
z=9     P=0.0000046
z=10    P=0.0000012

q=0.3
z=0     P=1.0000000
z=5     P=0.1773523
z=10    P=0.0416605
z=15    P=0.0101008
z=20    P=0.0024804
z=25    P=0.0006132
z=30    P=0.0001522
z=35    P=0.0000379
z=40    P=0.0000095
z=45    P=0.0000024
z=50    P=0.0000006
```

Solving for P less than 0.1%...

```
P < 0.001
q=0.10   z=5
q=0.15   z=8
q=0.20   z=11
q=0.25   z=15
q=0.30   z=24
q=0.35   z=41
q=0.40   z=89
q=0.45   z=340
```

12. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-work chain as proof of what happened while they were gone. They vote with their CPU power, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In *20th Symposium on Information Theory in the Benelux*, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In *Journal of Cryptology*, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time-stamping," In *Sequences II: Methods in Communication, Security and Computer Science*, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In *Proc. 1980 Symposium on Security and Privacy*, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

What IP Practitioners Should Know About Blockchain

Preston Byrne (Moderator)
Partner, Byrne & Storm, P.C.

Joshua Krumholz
Partner, Holland & Knight LLP

Jennifer Connors
Partner, Holland & Knight LLP

Holland & Knight

TECHNOLOGY & TELECOMMUNICATIONS ISG

THE INTERSECTION OF BLOCKCHAIN AND INTELLECTUAL PROPERTY

By: Joshua C. Krumholz, Partner, Holland & Knight

1. BLOCKCHAIN BASICS ARE NOT PROTECTABLE

1.1. ***Satoshi Nakamota (his/her true identity is unknown) released the first white paper on blockchain in 2008 entitled "Bitcoin: A Peer to Peer Electronic Cash System"*** [1]

1.2. ***Bitcoin itself was first offered to the open source community in 2009*** [2]

1.3. ***The information disclosed in those works is now dedicated to the public***

1.4. ***One cannot patent, for example, the broad concepts of a distributed ledger system or known cryptography techniques, both of which form the bedrock of blockchain***

1.5. ***But iterations and applications of that foundational technology are very much in play***

2. MANY APPLICATIONS FOR BLOCKCHAIN EXIST

2.1. ***While the use of blockchain is still in its infancy, its potential application is considerable***

2.2. ***Examples of blockchain applications presently being used include:***

2.2.1. **HSBC.** HSBC recently announced that, through its new blockchain platform, it has reduced the costs for its foreign exchange trades by one quarter.[3]

2.2.2. **JPM Coin.** JP Morgan has announced that it is the first US bank to successfully test its first cryptocurrency coin, the JPM Coin.[4]

2.2.3. **The Boomerang Project**. The Boomerang Project is a blockchain-based platform that enables a global system of online reviews, loyalty rewards programs and tipping based on verified transactions with a focus on the "gig economy" that connects contracted service providers ('workers') with consumers via an online/mobile app platform. Since the platform will be

---

[1] https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#34fbf9067bc4

[2] https://www.forbes.com/sites/bernardmarr/2018/02/16/a-very-brief-history-of-blockchain-technology-everyone-should-read/#34fbf9067bc4

[3] https://www.reuters.com/article/us-hsbc-blockchain/hsbc-forex-trading-costs-cut-sharply-by-blockchain-executive-idUSKCN1Q31MW?utm_source=applenews

[4] https://www.jpmorgan.com/global/news/digital-coin-payments

decentralized and will not be owned by any single entity, it is expected to eliminate or reduce the number of unverified reviews and restore trust in ratings.

2.2.4. **Tari Tickets**. Event ticketing normalizes a market where artists, teams, promoters and venues do not share in any of the ticket resale revenue, which is a large and growing market. Currently, ticketing platforms underinvest in innovation and do not prioritize improving the user experience for all stakeholders. Tari Tickets uses a blockchain platform to provide ticketing and marketing services to the global live events industry.

2.2.5. **The Codex Project.** Without a central title registry for arts and collectibles items, it is difficult to verify ownership and trace ownership history when establishing a collectible item's value. Forgeries cost the arts and collectibles industry $6 billion a year in losses. Right now, there are currently several methods of sale in the art and collectibles market, including private sales, live actions, and timed auctions. All of these methods lack a centralized title registry for each asset class (fine art, wine, jewelry, watches, collectible cars, etc.). Tracking, identifying, and confirming that an item is legitimate has been a challenge—yet that's critical to valuation. To address those issues, Codex has developed The Codex Protocol, which is a registry built on the blockchain that can show ownership, transmission history, and metadata like past appraisals, restoration records, or photographs. The Codex Protocol provides a way for everyone to verify ownership while keeping it decentralized and anonymous. The protocol maintains accurate title records, enables arts and collectible transactions, streamlines auction operations, all while maintaining privacy of participants.

2.3. ***But there are hundreds more, and each involves technical development that may or may not be the proper subject of IP protection***

3. EXAMPLES OF ALLOWED PATENTS

3.1. ***In total, the Patent Office has allowed over 260 patents related to blockchain***

3.2. ***Applications have risen steadily:***

3.2.1. In 2016, patent filings totaled 521[5]

3.2.2. In 2017, that number rose to 602[6]

3.2.3. Although it is hard to get precise numbers, in total, the number of applications has risen to over 1500

3.3. ***Chinese entities have constituted the largest number of filers, accounting for 56% of all applicants in 2017***[7]

3.4. ***Examples of subject-matter that has been allowed by the Patent Office includes:***

3.4.1. U.S. Patent No. 10,055,446 (Ensuring data integrity of executed transactions)

[5] https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead
[6] https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead
[7] https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead

3.4.1.1. The patent claims a central service provider that receives transaction data describing a first set of transactions, and receives transaction data from a primary recordation system describing a second set of transactions recorded by the primary recordation system. The primary recordation system can request and subsequently verify executed transactions and party positions with the central service provider that maintains the blockchain records. This permits the primary recordation system to maintain its role in servicing requests from various parties while the blockchain system of the central service provider provides additional transaction verification and confirmation. The elements of the claims directly involve an improvement in the field, specifically providing that the data state of the blockchain maintained by the central service provider can serve as a backup to a primary recordation system. As such, if a discrepancy arises (e.g. due to a missed, extra, or wrongful execution of a transaction or unauthorized change), the discrepancy can be readily identified and traced

3.4.2. U.S. Patent No. 9,875,510 (Consensus system for tracking peer-to-peer digital records)

3.4.2.1. The patent claims that it directly improves existing technological processes in digital object tracking and management. The disclosure describes a peer-to-peer consensus system and method for achieving consensus in tracking transferrable digital objects and preventing double spending by using a “most committed stake metric” to choose a single consensus transaction record. The most committed stake metric allows for a more complete and preserved history of block production and does not require block signers to sign a block unless the block references every prior block they’ve signed. Further, the most committed stake metric eliminates abandoned fork chains/blocks that are otherwise absent from the consensus chain, and facilitates detection and prevention in a fork resolution, which ultimately occurs via majority vote of stake. Further, participants can vote for fork chains automatically via transactions (which include a hash of a recent block from the consensus chain as known to the creator of the transaction). When there is a fork, the transactions will reference a recent block on the widest fork chain, and are only valid on the fork chain that they reference. Thus, these transactions add to the width of the already widest fork chain and resolve the fork to a single consensus chain

3.4.3. U.S. Patent No. 9,807,106 (Mitigating blockchain attack)

3.4.3.1. The patent claims a mechanism for detecting and mitigating threats to blockchain environments. It requires defining a transaction creation profile, submitting a transaction to the blockchain, which in turn causes the generation of a profiler data structure in the blockchain to generate profile transactions to be submitted to the blockchain according to the transaction creation profile, monitoring the blockchain to identify profile transactions and then comparing identified profile transactions with the transaction creation profile to detect a deviation from the transaction creation profile

4. THE ROLE AND IMPACT OF OPEN SOURCE SOFTWARE

4.1. ***Blockchain networks are typically built upon open source software, which can have a substantial impact on a developer's IP rights***

4.2. ***Open source software versus proprietary software***

4.2.1. The term "open source software" refers to software that is distributed in source code form. In source code form, the software can be tested, modified, and improved by people other than the developer who created the code in the first place

4.2.2. The term "proprietary" software refers to software that is distributed in object code form only. With proprietary software, the developer does not distribute the source code, but rather protects it as a trade secret. As a result, others are unable to modify, maintain, or have visibility into its software code base

4.3. ***Blockchain networks generally***

4.3.1. Public platforms

4.3.1.1. In a public network, each node of the network contains all transactions, the nodes are anonymous, and the participants are unknown to each other

4.3.1.2. Bitcoin and Ethereum are the leading public blockchain platforms[8]

4.3.2. Permissioned platforms

4.3.2.1. In a permissioned network, network members are vetted, unacceptable members are excluded, the nodes are not anonymous, and transactional information can be selectively disclosed to some, and not all, nodes

4.3.2.2. Hyperledger, Corda, and Enterprise Ethereum are the "big three" leading commercial, permissioned blockchain platforms[9]

4.4. ***The role of open source software licenses with blockchain platforms***

4.4.1. The software code bases for Bitcoin,[10] public Ethereum,[11] and Hyperledger,[12] and portions of the software code bases for Enterprise Ethereum[13] and Corda,[14] all consist of open source software

---

[8] R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038.
[9] R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038.
[10] *See* http://www.Bitcoin.org.
[11] L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing.
[12] "About Hyperledger," located at https://www.hyperledger.org/about.
[13] Enterprise Ethereum Alliance Specification Clears the Path to a Global Blockchain Ecosystem (May 16, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-specification-clears-path-global-blockchain-ecosystem/.

4.4.2. To use open source software, one must comply with the licensing requirements associated with that software, which will vary from one open source software to another. Each of the licenses, however, can have a substantial impact on a user's intellectual property rights

4.4.3. Generally, open source software licenses range from:

4.4.3.1. Permissive licenses, which allow licensees royalty-free and essentially unfettered rights to use, modify, and distribute applicable software and source code,[15] to

4.4.3.2. Restrictive, "copyleft" licenses, that place significant conditions on modification and distribution of the applicable software and source code

4.4.4. Two open source licenses are of particular import with regard to blockchain networks:

4.4.4.1. The General Public License, Version 3,[16] which governs large portions of the Ethereum code base,[17] and

4.4.4.2. The Apache 2.0 license[18] which governs open source software provided via the Hyperledger, Corda, and Enterprise Ethereum platforms[19]

4.5. *General Public License, Version 3 ("GPLv3") (Ethereum)*

4.5.1. GPLv3 is known as a strong copyleft license

4.5.2. To the extent that a developer incorporates GPLv3 code into his/her proprietary code, that developer must make his/her proprietary source code publicly available and at no charge, and may not restrict the use of that source code through copyright laws or otherwise

---

[14] "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md; Downloads: DemoBench for Corda 3.0, located at https://www.corda.net/downloads/.
[15] Bitcoin software, for example, is licensed under the permissive, MIT License. See http://www.Bitcoin.org; https://opensource.org/licenses/MIT.
[16] GPLv3 license, located at https://www.gnu.org/licenses/gpl-3.0.en.html .
[17] L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing. *See, e.g.*, Ethereum-sandbox License, located at https://github.com/ether-camp/ethereum-sandbox/blob/master/LICENSE.txt.
[18] Apache 2.0 license, located at https://www.apache.org/licenses/LICENSE-2.0.
[19] For Corda, *see* R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038; "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md. For Hyperledger, *see* Brian Behlendorf, "Meet Hyperledger: An 'Umbrella' for Open Source Blockchain & Smart Contract Technologies" (September 13, 2016) located at https://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies. Code contributed to the Enterprise Ethereum Alliance is generally made available under an open source license that mirrors the Apache 2.0 license, *see* Enterprise Ethereum Alliance Inc. Intellectual Property Rights Policy, available at https://entethalliance.org/join/.

4.5.3. Further, to the extent that the developer possesses patents that cover his/her proprietary code, the developer also must provide others with a royalty-free license to use the patents to the extent necessary to use the code

4.5.4. Finally, by using GPLv3 code, the developer cannot sue others for patent infringement to the extent they are using the GPLv3 code

4.5.5. In short, if a developer uses GPLv3 code, any code that he/she created that is based on the GPLv3 code becomes part of the public domain and free for anyone to use

4.6. ***Apache 2.0 license ("Apache") (Hyperledger, Corda and Enterprise Ethereum)***

4.6.1. Apache is more flexible than GPLv3

4.6.2. The impact can be similar to GPLv3 with respect to one's IP rights, but only if the developer affirmatively contributes its software to the maintainer of the Apache code at issue; in other words, it is not enough to simply use the open source software, the developer must affirmatively contribute whatever proprietary software he/she has created

4.6.3. In other words, the developer is free to use Apache code in his/her own proprietary code without a limitation of IP rights

4.6.4. In addition, a developer can still sue another Apache user for patent infringement; if he/she does, however, the developer's right to use the Apache code terminates

4.7. ***Based on the foregoing, one would assume that companies would stay away from restrictive usage, but that has not always been the case***

4.7.1. IBM, for example, has contributed code under the Apache license to the Hyperledger platform, and in turn is providing commercial Blockchain-as-a-Service (BaaS) offerings based on this platform using IBM's cloud infrastructure[20]

4.7.2. Microsoft has similar commercial offerings, based on Azure and the Enterprise Ethereum platform[21]

4.8. ***Making conscious choices***

4.8.1. The bottom line, however, is that the network that a company chooses can have an impact on that company's IP rights

4.8.2. Choosing a network is a technical one, typically made by IT professionals within the company

[20] IBM Blockchain, The Founder's Handbook: Your guide to getting started with Blockchain (Edition 2.0) located at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=28014128USEN.
[21] M. Finley, Getting Started with Ethereum using Azure Blockchain (January 24, 2018), located at https://blogs.msdn.microsoft.com/premier_developer/2018/01/24/getting-started-with-ethereum-using-azure-blockchain/

4.8.3. It is important for a company's legal department to be involved in that decision before significant investments are made in developing a blockchain product

5. THE THREAT OF (NON-PATENT) LITIGATION

5.1. ***Blockchain has the potential of being a highly disruptive technology***

5.1.1. Its potential applications include:

5.1.1.1. Financial transactions

5.1.1.2. Supply chain management

5.1.1.3. Real estate transactions and ownership

5.1.1.4. IP transactions and ownership

5.1.1.5. Health care

5.1.1.6. And many others

5.1.2. Most disruptive technologies generate litigation

5.2. ***Fraud cases***

5.2.1. Fraud cases have been by far the most prevalent so far. The vast majority, if not all, blockchain litigation has focused on cryptocurrency issues, and in particular where fraud has been committed in connection with specific cryptocurrency transactions.[22]

5.2.2. In addition to private lawsuits, five different federal regulators have brought suit, and state regulators have brought 46 separate administrative actions in thirteen states.[23]

5.3. ***Litigation by threatened stakeholders***

5.3.1. Disruptive technologies can make many enemies, namely the stakeholders that were once well-positioned but become displaced by the new technology.

5.3.2. Here the most obvious are third-party intermediaries that presently are necessary to mediate complex financial transactions, particularly trans-border transactions.

5.3.3. Another example involves logistics providers that mediate the complexities associated with supply chain management.

5.3.4. As changes are implemented, any blockchain adopter needs to consider the rights of these third parties, including their intellectual property rights, and make sure that those rights are addressed before litigation ensues.

5.4. ***Litigation by blockchain partners***

[22] www.blockchaincenter.com
[23] *Id.*

5.4.1. Because setting up a blockchain network is a complicated process, often involving many partners, disputes can arise between those partners and each other's rights.

5.4.2. Issues that should be preemptively considered include:

5.4.2.1. Understanding what intellectual property rights have been created through the construction of the blockchain network.

5.4.2.2. Establishing which rights belong to whom.

5.4.2.3. Understanding, per above, the impact that open source usage has on those rights.

5.4.2.4. Assessing what information can and cannot be shared by the members of the network.

5.4.2.5. Agreeing upon respective rights to administer, maintain, modify and operate the network, and credential new members.

6. THE THREAT OF PATENT LITIGATION

6.1. ***The largest threat, however, is the threat that has not yet arrived: the threat of patent litigation***

6.2. ***The present state of patent litigation***

6.2.1. After a number of years of heavy patent litigation, the size and amount of patent litigation matters has decreased in recent years

6.2.2. That reduction has been the result of many factors, but the key contributors are:

6.2.2.1. The creation of *inter partes review* proceedings, which have given defendants an opportunity to invalidate patents through the patent office, often staying proceedings in federal court during that process

6.2.2.2. Stricter requirements on proving damages, and the reversal by the Federal Circuit of many large district court awards

6.2.2.3. New defenses—in particular so-called *Alice* defenses—that may be interjected at the beginning of a case and that can result in an early dismissal

6.2.2.4. Patent pools and other organizations that acquire patents before they are acquired by patent trolls, and license those patents to their membership

6.2.2.5. Many of the most powerful patents in a broad range of industries already have been licensed

6.3. ***Blockchain may usher in a new wave of patent litigation***

6.3.1. History tells us that, notwithstanding the changes in the law discussed above and the constraints imposed by open source licenses, blockchain is likely to usher in a new wave of patent litigation

6.3.2. The reasons for that include:

6.3.2.1. Blockchain is creating a new set of patents, based on new technology, that have not been licensed

6.3.2.2. Blockchain technology likely will be used as fundamental building blocks, making the technology more valuable and damages more lucrative

6.3.2.3. Blockchain technology will be used in lucrative fields which, by association, will make blockchain patents more valuable

6.3.2.4. In a competitive landscape, certain companies will try to use their patents to keep competitors out of the marketplace

6.3.3. Patent trolls see the opportunity

6.3.3.1. A real indicator of the opportunity is the presence of patent troll investment in a field, which is the case with blockchain

6.3.3.2. Eric Spangenburg, a well-known founder of non-practicing entities ("NPEs"), has set up IPWE to collect and exploit blockchain patents, and Intellectual Ventures, a well-known and well-financed NPE, similarly is seeking to acquire and exploit patents in this area

6.4. ***Reasons to acquire patents in the field***

6.4.1. Offensive use

6.4.1.1. Blockchain technology is starting to become a crowded field. Some companies' entire business models are based on the creation of blockchain technologies. For those companies, acquiring and asserting patents may be the only way for them to effectively compete

6.4.1.2. Other companies may see an opportunity to monetize their R&D efforts through the licensing of their blockchain patent portfolio

6.4.2. Defensive use

6.4.2.1. As blockchain matures, patent leaders will emerge, and to avoid mutual destruction, they will enter into cross-licenses with each other

6.4.2.2. Other companies, in contrast, will try to enter the industry without a proper patent portfolio, and may find significant barriers to entry if the patent leaders seek to assert their right to exclude those other companies from using their patented technology

6.4.2.3. So the bottom line is that any major player in the blockchain field needs patents to at least cross-license with its major competitors

6.4.2.4. And acquiring patents can also stop another company from patenting the same idea and asserting it against you

6.5. ***Strategies for limiting patent litigation exposure include:***

6.5.1. **Join patent pools.** Patent pools are membership-based organizations that acquire patents, or take licenses on patents, for the benefit of their members

6.5.2. **Actively enter into cross-license agreements.** If a company has an existing portfolio, consider approaching other major players in the blockchain field to enter into cross-licenses with those companies

6.5.3. **Monitor patent application and allowed patents.** Review patent applications as they are published (18 months after filing) and when patents issue to take preventative action on those patents

6.5.4. **Consider design-arounds where available.** To the extent a company identifies potentially problematic patents or applications, an option for it is to "design around" the problematic patent

6.5.5. **Be prepared to file IPRs.** To the extent a company finds a problematic patent, one option is to file an IPR with the Patent Office to try to invalidate the patent

6.5.6. **Prepare open source defenses.** At a minimum, investigate whether the lawsuit violates an open source license agreement

6.5.7. **Attack the patents on *Alice* grounds.** If a company ends up in litigation, it still may be able to terminate that litigation early by filing an *Alice* motion because the concept of blockchain itself is an abstract idea, and not patentable as such

6.5.8. **Assert counterclaims.** As discussed above, it is important for a company to acquire its own patent portfolio. If successful in doing so, and if sued by a practicing company, that company may be able to assert its own claims of patent infringement. Doing so typically makes it easier to resolve a dispute in its early stages

7. THE ROLE OF BLOCKCHAIN STANDARDS

7.1. ***Industry standards***

7.1.1. Industry standards refer to technical specifications that industry members agree to use in their products.

7.1.2. Industry standards are collaboratively developed through Standards Setting Organizations (or "SSO"). Periodically, the SSO will hold meetings where industry players will propose and debate differing proposals regarding how a technology should operate

7.1.3. Decisions regarding proposals, and the final technical specifications that stem from them, are reached by consensus by the participants

7.2. ***Blockchain standards are presently being created:***

- The International Standards Organization ("ISO") has formed Technical Committee 307 ("ISO/TC 307") to consider blockchain and distributed ledger technologies.[24]

- The Institute of Electrical and Electronics Engineers ("IEEE") has formed two blockchain groups: (1) Project 2418 to develop a standard framework for the use of blockchain in Internet-of-Things applications;[25] and (2) Project 825 to develop a guide for interoperability of blockchains for energy transaction applications.[26]

- The Blockchain in Transportation Alliance ("BiTA") is focused on the use of blockchain in freight payments, asset history, chain of custody, smart contracts and other related goals.[27]

- The Enterprise Ethereum Alliance recently released an architecture stack designed to provide the basis for an open-source, standards-based specification to advance the adoption of Ethereum solutions for commercial, permissioned networks (referred to as "Enterprise Ethereum").[28]

7.3. ***Lessons from the wireless industry***

7.3.1. Standards have had a dramatic effect, both positive and negative, on the wireless industry

7.3.2. Industry standards have essentially allowed the wireless industry to blossom by:

7.3.2.1. Ensuring compatibility between and among devices and equipment

7.3.2.2. Creating a framework that optimizes the best technologies

7.3.2.3. Creating a safe framework for investment and adoption

7.3.2.4. Allowing for better planning with more accurate forecasts

7.3.3. There are disadvantages to standards as well:

7.3.3.1. To a degree, they can level out the playing field

7.3.3.2. Alternative standards often compete with each other before adoption, and companies can invest in the wrong standard

[24] https://www.iso.org/committee/6266604.html.
[25] http://standards.ieee.org/develop/project/2418.html.
[26] http://standards.ieee.org/develop/project/825.html.
[27] https://bita.studio.
[28] Enterprise Ethereum Alliance Advances Web 3.0 Era with Public Release of the Enterprise Ethereum Architecture Stack (May 2, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-advances-web-3-0-era-public-release-enterprise-ethereum-architecture-stack/; https://entethalliance.org/wp-content/uploads/2018/05/EEA-TS-0001-0-v1.00-EEA-Enterprise-Ethereum-Specification-R1.pdf.

7.3.3.3. Companies are held captive to certain required features and functions, and may need to use others' patents to enable those features and functions

7.3.3.4. SSOs are less nimble than individual companies to make technical changes

7.3.4. There are good reasons for the blockchain industry to invest in the creation of industry standards. Blockchain is based on networks that are large enough—*i.e.* have enough nodes—to create reliability. As such, interoperability and scalability are important. Standardization of blockchain elements can be an important tool in achieving those goals

7.3.5. The standardization process often involves competing visions. Certain companies will advance one approach, and other companies will advance a different approach. That advocacy typically is based on a good faith belief, but it also arises from investments that companies make in their technology

7.3.6. A meaningful standardization process contains both risk and opportunity because no company wants to be make the wrong bet and become the Betamax of blockchain technology. Companies therefore need to be thinking hard about the competing standards that are being created and what role they wish to play in that creation. An entirely passive role can result in other thought leaders seizing the marketplace, but too aggressive a role can lead to massive investments that are not adopted by the marketplace as a whole

7.4. ***The impact of industry standards on blockchain IP***

7.4.1. From an IP perspective, the creation of standards can have a significant impact

7.4.2. If a company's patented technology is adopted into a standard, it becomes a "standards-essential" patent, meaning that everyone in the industry must practice it to comply with the standard

7.4.3. In that situation, the company holding the patent is compelled to license the patent to others under FRAND (fair, reasonable and non-discriminatory) terms, which of course can be a matter of much debate

7.4.4. And many patent trolls will claim that their patents are essential to compliance with a standard, which can change the complexion of a litigation

Blockchain & Cryptocurrency Regulation

2019

First Edition

Contributing Editor
Josias Dewey

glg global legal group

CONTENTS

Country chapters

Blockchain and intellectual property: A case study

Joshua Krumholz, Ieuan G. Mahony & Brian J. Colandreo
Holland & Knight LLP

Introduction

As discussed elsewhere in this book, blockchain has the potential for transformational change. Like most transformational technologies, its development and adoption are laden with intellectual property ("IP") issues, concerns and strategies. Further, given the potentially wide-ranging impact of blockchain technology, the public and private nature of its application, and the prevalent use of open source software, blockchain raises particularly unique IP issues.

The purpose of this chapter is to help the practitioner identify some of the issues that may affect blockchain development and adoption. We address these issues as they may relate to a company's creation of its own IP, and as they may relate to efforts by others to assert their IP against a company. We discuss the issues in the context of the hypothetical scenario discussed below.

The hypothetical transaction

Although many sectors stand to benefit from the use of blockchain technology, the financial and supply chain management sectors may be among the first to benefit. For purposes of discussion, this chapter focuses on the financial sector, and in particular the following hypothetical:

> *A U.S. company is building a new platform using distributed ledger technology for its syndicated loan transactions. Many participants are involved in a typical transaction serviced by the platform, including borrowers, lenders, an administrative agent, credit enhancers and holders of subordinated debt. The platform that the company is building employs smart contracts to effectuate the functionality over a permissioned (private) network with several hundred nodes in the network.*

Our hypothetical company, as noted, has chosen to deploy its solution via a permissioned network. A blockchain developer has two broad options in this regard. First, the developer could select a public blockchain network for its platform. In a public network, each node contains all transactions, the nodes are anonymous, and participants are unknown to each other. Second, the developer could select a permissioned network (as our hypothetical company has). In a permissioned network, the network owner vets network members, accepts only those that it trusts, and uses an access control layer to prevent others from accessing the network. Unlike the nodes on a public network, the nodes on a permissioned

network are not anonymous. In addition, a permissioned network can be structured so that specified transactions and data reside only on identified nodes, and are not stored on all nodes in the network.[1] In certain commercial transactions, participants must be known to each other in order to meet regulatory requirements, such as those designed to prevent money laundering. In these situations, a network of anonymous nodes would not be compliant.

Our hypothetical company has selected a permissioned network, we can assume, to obtain these benefits. This selection comes with costs, however, and the company will lose the benefit, for example, of validating a transaction over the full multitude of distributed nodes in a public blockchain network, and the assurances of immutability that that provides.

The blockchain patent landscape

Since Satoshi Nakamoto published the Bitcoin whitepaper in 2008,[2,3] the number of blockchain patent applications has steadily risen. In 2016, applicants filed 521 patents related to blockchain technologies in the United States.[4] In 2017, the number of filings rose to 602.[5] Notably, Chinese entities filed the greatest number of U.S. blockchain patent applications in 2017, accounting for 56% of all filed applications.[6] Applications for blockchain patents filed by U.S. entities accounted for 22% during that same period.[7]

The United States Patent and Trademark Office has begun to issue blockchain patents based on these filings. Below is a breakdown of the largest holders of blockchain patents as of early 2018.[8]

Entity	Industry	No. of blockchain patents
Bank of America	Finance	43
MasterCard	Finance	27
IBM	Technology	27
Fidelity	Finance	14
Coinbase	Finance	13
World Award Foundation / World Award Academy / AMobilePay, Inc.	IP holding	12
TD Bank	Finance	11
402 Technologies S.A.	IP holding	10
Accenture	Technology	9
Dell	Technology	8

Because blockchain technology assists in the efficient and secure transfer of assets, it is no surprise that the financial industry currently dominates the blockchain patent space. Technology companies like IBM[9] and Dell[10] also are utilising blockchains to improve existing technologies and processes, including supply chain and digital rights management. The IP holding companies, meanwhile, presumably seek patents solely to monetise them.

What can be protected?

Only new and novel ideas may be patented

Ideas that already are in the public domain may not be patented, and much of blockchain technology falls into that category. As discussed elsewhere in this book, a blockchain is a distributed ledgering system that allows for the memorialising of transactions in a manner that is not easily counterfeited, is self-authenticating, and is inherently secure. The

basic concept of a blockchain may not be patented. A ledgering system that records such transactions, employs multiple identical copies of the ledgers, and maintains them in separate and distinct entities, similarly may not be patented as a new and novel idea. Blockchain technology also uses cryptography. Known cryptography techniques, even if used for the first time with blockchain, also are not likely to be patentable unless the combination resulted from unique insights or efforts to overcome unique technical problems.

Anyone is generally free to use these concepts and, as such, they are not patentable. So what is left that can be protected? Only novel and non-obvious ways to use the above-described blockchain distributed ledger system may be protected. For example, the traditional banking industry utilises central banks and clearing houses to effectuate the transfer of money between entities, which often results in significant delay to complete the transactions. With access to overnight shipping, real-time, chat-based customer service, and social networks allowing for the live-video conferencing of multiple parties positioned around the globe, it is understandable that today's consumer could be disillusioned with the pace at which financial transactions move through the traditional banking industry.

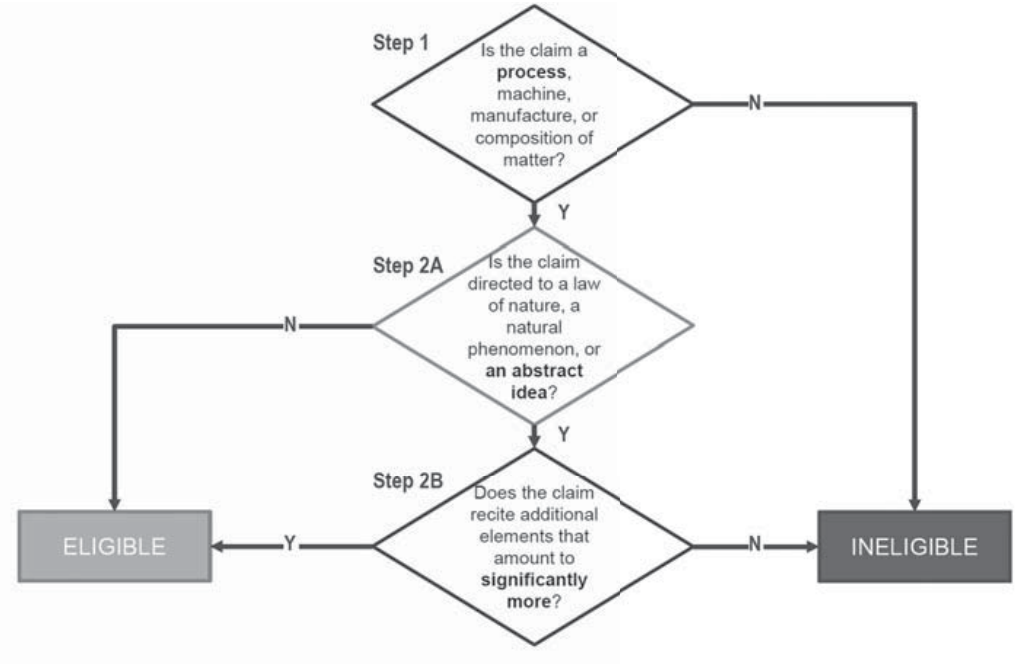
Accordingly, various companies and entities are devoting considerable time and resources to refining and revising the manner in which the traditional banking industry effectuates such monetary transactions. Entrepreneurial companies are inventing unique systems for effectuating asset transfers between banking entities that are memorialised via the above-described blockchain distributed ledgering system, as well as unique systems for expanding the utility of distributed ledgers via remote (and cryptographically-secured) content defined within the distributed ledgers. These improvements, as a general proposition, build and improve upon the foundational blockchain technology. Such an improvement could take the form, for example, of an application deployed on the "foundation" of the Hyperledger platform, and designed to verify the identity of participants in the hypothetical company's permissioned network, or to create audit trails for transactions on this network. It is these incremental improvements that potentially may be patentable. And it is in this area that our hypothetical company should be focusing its patenting efforts.

The *Alice* decision

Obtaining a patent by our hypothetical company also faces another obstacle. As explained by the Supreme Court in *Alice Corp. v. CLS Bank Int'l*, to be patentable, a claimed invention must be something more than just an abstract idea.[11] Rather, it must involve a technical solution to a specific problem or limitation in the field. In the *Alice* case, for example, a computer system was used as a third-party intermediary between parties to an exchange, wherein the intermediary created "shadow" credit and debit records (*i.e.*, account ledgers) that mirrored the balances in the parties' real-world accounts at "exchange institutions" (*e.g.*, banks). The intermediary updated the shadow records in real time as transactions were entered, thus allowing only those transactions for which the parties' updated shadow records indicated sufficient resources to satisfy their mutual obligations.

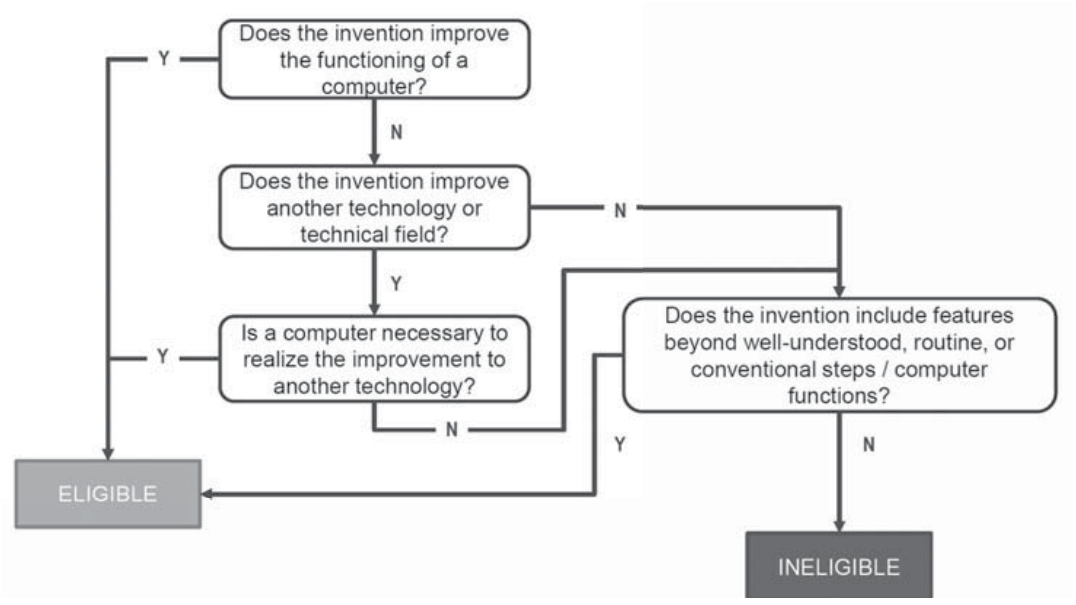
The Supreme Court held that, "[O]n their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk." The Court went on to explain that "[T]he concept of intermediated settlement is a fundamental economic practice long prevalent in our system of commerce." The Court then explained that such basic economic principles could not be patented, even if implemented in software or in some other concrete manner, because abstract ideas are not themselves patentable. Allowing patents on abstract ideas themselves, the Supreme Court explained, would significantly restrict and dampen innovation.

The following flowchart defines the manner in which the patentability of subject matter should be analysed with respect to the *Alice* decision:



As such, basic concepts, even as they relate to blockchain, may not be patentable. So our hypothetical company must present more than just basic, economic principles in order to get a patent. It must, for example, claim specific improvements to the functioning of a computer, improvements to other, related technology, effect a transformation of a particular article to a different state or thing, add a specific implementation that is not well-understood, routine or conventional, or add unconventional steps that confine the claim to a particular useful application.

The following flowchart may be utilised when assessing the patentability of subject matter with respect to the *Alice* decision:



If the *Alice* decision taught practitioners anything, it is that IP law is continuously changing. Accordingly, just as a sound investment plan requires a diversified securities portfolio, a sound IP strategy requires a diversified IP portfolio. Therefore, companies should not put all of their proverbial eggs into one IP basket. For example, if a company was in the "intermediated settlement" space and all they owned were U.S. utility patents, the *Alice* decision would have been devastating to it.

Accordingly, companies should include utility patents in their IP portfolio. But the prudent company also would include design patents (for protecting, *e.g.*, user interfaces); trade secrets (for protecting, *e.g.*, backend algorithms that are not susceptible to reverse engineering); trademarks (for protecting the goodwill associated with the products produced by the company); service marks (for protecting the goodwill associated with the services provided by the company); copyrights (for protecting software code, and/or the expression of a concept or an idea); and various IP agreements (*e.g.*, employment agreements, development agreements, and licensing agreements). The best IP portfolio for our hypothetical company, therefore, should resemble a quilt that is constructed of various discrete components (utility patents, design patents, trade secrets, trademarks, service marks, copyright, and IP agreements) that are combined to provide the desired level of IP coverage.

The assertion and defence of patent litigation

The threat of patent litigation

Just a few years ago, patent litigation was ubiquitous. Identifying an unique market opportunity, non-practising entities ("NPEs"), also known as "patent trolls", sprung up, aggregated patents, targeted specific industries, and monetised those patents either through threats of litigation or actual lawsuits. One sector that was the subject of this attack was the telecommunications industry. Beyond a number of competitor-versus-competitor suits (such as *Apple v. Samsung*), large, sophisticated NPEs also arose that did not make a product or sell a service. Rather, they purchased telecom patents, created portfolios, and engaged in litigation campaigns to force companies to pay royalties on those patents. Often, if a NPE had a large enough portfolio, a telecom company would enter into a licence agreement to license that portfolio for a defined period of time, often five years.

In the last few years, patent litigation has waned. Due to Congress's creation of *inter parties review* ("IPR") proceedings, stricter requirements on proving damages, member organisations that acquire patents and offer licences to their members, restrictions on where patent lawsuits may be filed, and new defences that allow patents to be invalidated more easily in the early stages of litigation, patent litigation is no longer the economic opportunity it once was. While competitors still will engage in patent litigation to preserve (or attack) their relative positions in the marketplace, NPEs have found that this changing landscape has made patent litigation financially less rewarding. To be sure, such patent litigation still exists. Indeed, new lawsuits are filed daily. The number and threat of those lawsuits has greatly diminished, however, and the value of patents generally has diminished as well.

Market changes, of course, can create new incentives for initiating patent litigations, and the increased role of blockchain technology is likely to bring about one of those changes. To the extent blockchain technology becomes prevalent, it is likely to result in substantially increased patent litigation, both between competitors and between NPEs and practising companies. The reasons for this potential change are several:

- In a competitive landscape, certain companies – specifically those technology companies solely directed toward creating blockchain products – must use their patents to keep competitors out of the marketplace.
- Blockchain is ushering in a new set of patents, based on new technology, that have not been licensed.
- Blockchain technology will be used in lucrative fields which, by association, will make blockchain patents more valuable.
- Blockchain technology likely will be used as fundamental building blocks, making the technology more valuable and damages more lucrative.

Certainly, NPEs see the opportunity. Eric Spangenburg, a well-known founder of NPEs, has set up "IPwe" to collect and exploit blockchain patents, and Intellectual Ventures, a well-known and well-financed NPE, similarly is seeking to acquire and exploit patents in this area.[12] And our hypothetical transaction platform reflects this opportunity. If our hypothetical company builds blockchain technology into the basic building blocks of its transactions, and its transactions form the basic building blocks of its business, then it stands to reason that the technology underlying those activities has significant value.

Offensive and defensive uses of patent rights

When entering into this new technical field, therefore, it is critical that our hypothetical company understand the patent landscape. Are there so many patents that they create a barrier to entry? Are other companies actively applying for patents? If so, are they doing so to block others or require licensing fees, or are they doing so merely for defensive purposes? Understanding and properly predicting this landscape may be the difference between a successful and a failed endeavour.

Broadly speaking, the strategic use of patent rights can be categorised as offensive or defensive (or a mix of the two). These strategies are discussed in greater detail below.

- *Offensive uses of patent rights*

  From an offensive perspective, the holder of a patent gains the right to exclude others from making, using or selling the invention.[13] An offensive patent holder therefore has the ability to block all others from utilising its patented inventions. In an emerging technical field like blockchain, patent-filers typically have a more open landscape of new solutions to discover and claim. Because of the patent holder's right to exclude, each solution it is able to patent can block competitors from utilising that solution in their own products or services, unless granted permission.

  For our hypothetical company, if the patented technology allows for a more efficient and secure transaction, our hypothetical company may want to exclude others from using that technology, giving the hypothetical company a competitive advantage in the marketplace. If our hypothetical company does not wish to exclude competitors, it may instead allow other companies to use its patented technology, but demand that they pay reasonable royalties for that use, perhaps to help defray research-and-development costs or to create an alternative revenue stream.

  It is not enough, however, for the offensive patent holder to file and receive issued patents. The offensive patent holder must affirmatively enforce its patent rights, and make sure that those patent rights are not encumbered by open source licences, *per* our discussion below in "The impact of open source software", or by FRAND licensing obligations, *per* our discussion below in "The role of industry standards". Enforcement requires monitoring for activities that may infringe the patent holder's claims, demanding

that others halt infringing activities and, if necessary, instituting litigation to halt the activities by and/or receive reasonable compensation for those activities.

Our hypothetical company also may seek to develop income streams from its patent portfolio. By enforcing its patent rights, the offensive patent-holder may force competitors to take and pay for licences. These licences may provide income to the offensive patent-holder as a single lump sum, where the licensee pays for its license upfront, or as a running royalty, where the licensee pays a percentage of the revenue generated by its products in the marketplace.

- *Defensive uses of patent rights*

  Rather than affirmatively asserting patents, the defensive patent-holder uses them as a hedge against other potential claims against it. Thus, in our hypothetical, where the hypothetical company is building a platform and cannot have that platform's use interrupted, the hypothetical company needs to build up as many defences against a claim of patent infringement as possible. By having its own portfolio, our hypothetical company may be able to deter competitors from a lawsuit against it, because that competitor knows that it may face claims against it if it brings a patent infringement action.

  A defensive strategy, if timely performed, also can block others from securing patents that later can be asserted against it. That is, in fact, the precise strategy of Coinbase's patent filings. By filing for as many patents as possible in the blockchain field, Coinbase hopes to take away patent rights from non-practising entities, which they could otherwise assert against Coinbase.[14]

  Ultimately, as blockchain matures, players in the field will tend to take several forms. Patent leaders will emerge, and to avoid mutual destruction, they will enter into cross-licences with each other. Other companies will try to enter the industry without a proper patent portfolio, and may find significant barriers to entry if the patent leaders seek to assert their right to exclude those other companies from using their patented technology. And then there will be companies that simply acquire patents for the purpose of asserting them. They will create transaction costs, but should not bar entry into the marketplace.

* * *

So, for our hypothetical company, it needs to look at the long-term. Is it creating a platform of critical importance, but leaving itself vulnerable to its competitors? Is it fully taking advantage of its hard work and innovation by protecting the original and novel concepts that it created? Will it find itself blocked by aggressive competitors that are aggregating important patents? All of these questions must be addressed at the same time that our hypothetical company is investing in its technological improvements, and seeking to attract entities and (perhaps) developers to join and participate in its newly created blockchain network.

Strategies for limiting patent litigation exposure

The threat of patent litigation in the blockchain field is real. So how can our hypothetical company limit potential liability? There are several steps that it can take:

- **Open source defences**. At a minimum, if a claim is asserted, our hypothetical company needs to consider whether that claim is blocked or barred by open source restrictions. In addition, our company also should be deliberating carefully on its own open source strategy, and how the use of open source software impacts its potential defences and assertion rights.

- **Actively enter into cross-licence agreements**. If our hypothetical company has acquired a significant patent portfolio, then it may want to approach other major players in the blockchain field and seek to enter into cross-licences with those companies. This approach allows companies to compete based on the quality of their product or service, rather than engage in a damaging patent war.
- **Join patent pools**. In certain industries, particularly telecommunications, companies have arisen to help combat NPEs. These companies are membership-based organisations, whereby companies pay a fee for a licence to all patents held by the company. The company's typical approach is to acquire patents, or take licences on patents, for the benefit of its members. The goal of these organisations is to charge a reasonable fee for a licence to a broad-based portfolio.
- **Monitoring patent application and allowed patents**. While there are many blockchain patents and patent applications, they number in the hundreds, not the thousands. As such, if committed, our hypothetical company can review patent applications as they are published (18 months after filing) and when patents issue. Doing so allows a company to identify potentially problematic patents. The downside of such an approach, however, is that such monitoring may become discoverable in a patent litigation, and perhaps can be used as evidence of knowing (wilful) infringement.
- **Consider design arounds where available**. To the extent our hypothetical company identifies potentially problematic patents or applications, an option for it is to "design around" the problematic patent. In other words, our hypothetical company can analyse the particular elements that make up the invention, and eliminate one or more of those elements in its product in order to avoid practising the patent.
- **Be prepared to file IPRs**. If our hypothetical company finds a problematic patent, one option is to file an IPR with the Patent Office to try to invalidate the patent. Our hypothetical company can take that step even if no lawsuit has been filed against it. Deciding to do so requires an assessment of the likelihood that the patent can be invalidated and the cost associated with that process, but that cost will always be substantially less than the cost of patent litigation.
- **Be prepared to attack the patents on *Alice* grounds**. If our hypothetical company ends up in litigation, it still may be able to terminate that litigation early by filing an Alice motion, discussed more fully in the section, "Defensive uses of patent rights", above. The concept of blockchain itself is an abstract idea, and not patentable as such. To have a valid blockchain patent, the claimed idea must identify some technical problem in the field and provide some specific technical solution to that problem. Without providing something sufficiently concrete, our hypothetical company may be able to invalidate the asserted patent early in the litigation process.
- **Assert counterclaims**. As discussed above, it is important for our hypothetical company to acquire its own patent portfolio. If successful in doing that, and if sued by a practising company, our hypothetical company may be able to assert its own claims of patent infringement. Doing so typically makes it easier to resolve a dispute in its early stages.

The impact of open source software

The term "open source software" refers to software that is distributed in source code form. In source code form, the software can be tested, modified, and improved by entities other than the original developer. The term "proprietary" software refers to software that, in

contrast, is distributed in object code form only. The developer of proprietary software protects its source code as a trade secret, and declines to allow others to modify, maintain, or have visibility into its software code base. Proponents of open source software state that the structure fosters the creation of vibrant – and valuable – developer communities, and leads to a common set of well tested, transparent, interoperable software modules upon which the developer community can standardise.

Open source software is ubiquitous in blockchain platforms. The software code bases for Bitcoin,[15] public Ethereum,[16] and Hyperledger,[17] and portions of the software code bases for Enterprise Ethereum[18] and Corda,[19] all consist of open source software. Bitcoin and Ethereum are the leading public blockchain platforms, and Hyperledger, Corda, and Enterprise Ethereum are the "big three" leading commercial, permissioned blockchain platforms.[20] Accordingly, if our hypothetical company wishes to leverage solutions that rely on software from any of these leading platforms, it must consider the impact of the licences that govern this software.

The open source community has developed a number of licences, and these range from: (a) permissive licences, that allow licensees royalty-free and essentially unfettered rights to use, modify, and distribute applicable software and source code;[21] to (b) restrictive, so-called "copyleft" licences, that place significant conditions on modification and distribution of the applicable software and source code. Two open source licences are particularly relevant to our hypothetical company: the General Public License version 3 ("GPLv3"),[22] because this licence (and variants) governs large portions of the Ethereum code base,[23] and the Apache 2.0 licence (the "Apache License"),[24] because this licence governs open source software provided via the Hyperledger, Corda, and Enterprise Ethereum platforms.[25] Each of these licences embodies a "reciprocity" concept that our hypothetical company must consider.

GPLv3 is known as a "strong" copyleft licence. The licence functions as follows: assume a developer is attracted to a software module subject to GPLv3, and incorporates this module into proprietary software that he or she then distributes to others. To the extent the developer's proprietary software is "based on" the GPLv3 code,[26] the developer is required to make his or her proprietary code publicly available in source code form, at no charge, under the terms of GPLv3. This requirement will remove trade secret protection embodied in the proprietary code, as well as the developer's ability under copyright law to control the copying, modification, distribution, and other exploitation of its software.[27] This licence, therefore, has a significant impact on the developer's trade secret and copyright portfolios.

GPLv3 also has a significant impact on the developer's patent portfolio. The licence obligates the developer to grant to all others a royalty-free licence to patents necessary to make, use, or sell the Derivative Code.[28] Finally, simply by distributing GPLv3 code, without modification, the developer agrees to refrain from bringing a patent infringement suit against anyone else using that GPLv3 code.[29] In sum, the structure of GPLv3 reflects a strong "reciprocal" concept: if a developer wishes to incorporate open source software into its code base, it must reciprocate by contributing that code base (and all needed IP rights) back to the community. As noted above, the Ethereum code base is licensed predominantly under GPLv3. Therefore, our hypothetical company should use caution in relying on Ethereum code.

Our hypothetical company should also consider the impact on its IP portfolio of relying on Hyperledger, Corda, and Enterprise Ethereum code. The Apache licence (or an equivalent) governs large portions of these code bases. For our hypothetical company, although the Apache licence has reciprocal features, it is considerably more flexible than GPLv3. The

Apache licence impacts a developer's rights to its software under patent, trade secret, and copyright law in a manner similar to GPLv3;[30] however, these impacts only arise where the developer affirmatively contributes its software to the maintainer of the Apache code at issue. The structure functions with respect to patents as follows: if a patent owner contributes software to an Apache project, the Apache licence restricts the owner from filing a patent infringement claim against any entity based on that entity's use of the contributed software. If the owner does bring such a suit, the owner's licence to the Apache code underlying its contribution terminates.[31] The licence thus has a reciprocal structure: a patent owner cannot benefit from Apache-licensed software while suing to enforce patents that read on its contributions to the Apache software community. If the developer, however, decides not to contribute its code to an Apache project, the developer remains free to incorporate Apache code into its proprietary code base, and commercialise this code without obligation to the Apache open source community. The Apache licence, therefore, provides developers with considerable flexibility.[32]

This flexibility may present strong value to our hypothetical company. It would permit the company, for example, to leverage existing Apache-licensed software from the Hyperledger, Corda, and Enterprise Ethereum code bases in order to develop its new platform and applications, and would give the company full control over whether and to what extent it wishes to encumber its intellectual property portfolio with open source obligations.

Based on the above, it might appear that our hypothetical company would take extreme steps to avoid GPLv3 code (or other strong copyleft code) and would never contribute code to an Apache project. This, however, has not been the case. A number of entities have contributed code under the Apache licence, for example, in order to encourage developers and users to adopt the permissioned commercial network that implements this code.[33] Our hypothetical company will similarly want to consider the potential benefits of seeking to create a vibrant developer and user community using an "open" approach to its intellectual property portfolio, and potentially contributing code under an appropriate open source software licence. In any event, open source software licences and licensing techniques play a key role in blockchain technology, and our hypothetical company will want to carefully consider these licences and techniques in its IP strategy.

The role of industry standards

Background

Industry standards refer to a set of technical specifications that a large number of industry players agree upon to use in their products.[34] Industry players collaboratively develop these technical specifications in a Standards Setting Organization (or "SSO"). Periodically, the SSO will hold meetings where participants, often scientists and engineers, representing industry players will propose and debate differing proposals regarding how a technology should operate. Decisions regarding proposals, and the final technical specifications that stem from them, are reached by consensus by the participants.

Current efforts to standardise blockchain technology

Several organisations have begun standardising a variety of blockchain technologies:

- The International Standards Organization ("ISO") has formed Technical Committee 307 ("ISO/TC 307") to consider blockchain and distributed ledger technologies.[35]
- The Institute of Electrical and Electronics Engineers ("IEEE") has formed two blockchain groups: (1) Project 2418 to develop a standard framework for the use of

blockchain in Internet-of-Things applications;[36] and (2) Project 825 to develop a guide for interoperability of blockchains for energy transaction applications.[37]

- The Blockchain in Transportation Alliance ("BiTA") is focused on the use of blockchain in freight payments, asset history, chain of custody, smart contracts and other related goals.[38]
- Hyperledger is a blockchain standard project and associated code base hosted by the Linux Foundation that focuses on finance, banking, Internet-of-Things and manufacturing.[39]
- The Enterprise Ethereum Alliance recently released an architecture stack designed to provide the basis for an open-source, standards-based specification to advance the adoption of Ethereum solutions for commercial, permissioned networks (referred to as "Enterprise Ethereum").[40]

Advantages and disadvantages of standards

- *Advantages of using and contributing to industry standards*

  There are several advantages to using standards that benefit an industry at-large:

  - **Ensures product compatibility** – With a standard in place, any vendor can develop a product that will be compatible with other products in the industry.
  - **Stronger technology** – Technical specifications created with the input of many industry players tend to result in stronger overall technologies. In theory, the best ideas should emerge from the process and become industry standards that benefit both vendors and consumers.
  - **Shifts competition from the standardised technology to implementation** – Standardisation allows industry players to avoid competition with regard to the standardised technology, and instead shift their focus to developing the best implementation of the remaining technology. Entities that participate in the standard-setting process are obligated to disclose patents that are essential for implementing the standard, and to provide licences to these patents on fair, reasonable, and non-discriminatory terms (so-called "FRAND" terms). These FRAND obligations ensure that all implementers bear the same licensing burden as regards patents essential to the standard.
  - **Greater likelihood of wide adoption** – Approval by many industry players makes the standardised approach a "safer bet" for technology adopters and investors.

  Contributing to SSOs also yields several benefits to individual participants. First, a participating company gains visibility into what comes next in their industry. For example, a software vendor for a syndicated loan blockchain platform could observe the emerging form and content of the blockchain's smart contracts and begin to steer its internal development toward efficiently processing those contracts. Second, a participating company has the opportunity to guide the standardisation process. For example, steering the SSO toward smart contracts that reference cloud-based digital documents would be advantageous for a vendor with a strong cloud-based solution in place.

- *Disadvantages of using and contributing to industry standards*

  There are disadvantages to employing industry standards as well. First, a company loses control over certain aspects of the technology. Instead of developing technology in isolation, our hypothetical company could be at the whim of the industry and its own competitors. Second, a company could develop its own technology that wins

over others' in the marketplace. Good-faith participation in an SSO implies that a company will contribute its best, most valuable ideas to the SSO instead of applying them solely to its own products. But the prize for developing better technology than the SSO's participants, and not contributing it, is alluring: a lucrative monopoly on the best technology. Third, an SSO is less nimble than an individual company because changes to industry standards takes consensus of many parties, which in turn takes time. Finally, by participating in the SSO process, the company will place FRAND obligations on any patents in its portfolio that are essential for purposes of implementing the standard.

Lessons from wireless telecommunications industry standards

Blockchain technology is a relatively new field, and SSOs are only starting to form to develop blockchain standards. Many companies are now deciding whether to join a blockchain SSO or pursue their own solutions. Another technical field, telecommunications, and the history of its standardisation activities, provides a good example of the advantages and disadvantages of pursuing industry standards or deciding to go it alone.

In order for a phone to access a carrier's wireless network, it must know how to communicate with the carrier's network. Telecommunications standards dictate how that communication proceeds. By adhering to the telecommunications standard, a manufacturer can ensure that its phone can operate on any carrier's wireless network that also follows that standard.

In the 1980s, the European "first generation" wireless telecommunications market was fractured by a handful of standards marked by national or regional boundaries. Scandinavia used a standard called "NMT"; Great Britain used "TACS"; Italy used "RTMS" and "TACS"; France used "RC2000" and "NMT"; and Germany used "C-Netz".[41] Using this hodgepodge of telecommunications standards meant that a German's phone would not work during her vacation to France, and an Englishman's phone would not work in Scandinavia.[42] Manufacturers for both phones and network infrastructure were likewise geographically constrained. These manufacturers would typically only research and develop products for specific European regions. What resulted were regional monopolies for those manufacturers, but with low subscriber rates and little opportunity to compete in foreign markets where their technology would be inoperable.[43]

Mindful of these issues with the first generation wireless telecommunications standards, phone and infrastructure manufacturers from around Europe (and indeed around the world) came together to develop a pan-European, "second generation" standard within the European Telecommunications Standards Institute ("ETSI") SSO. These manufacturers sent their best scientists and engineers to ETSI to ensure that this emerging standard would meet wireless subscribers' and carriers' needs. The result of their work was the Global System for Mobile communications ("GSM"), which was the *de facto* wireless standard throughout Europe and parts of the United States from 1992 through 2002. During that period, manufacturers would compete to develop better phones or network equipment, all the while maintaining compliance with the GSM standard. As a result, equipment developed in Sweden or Finland could be sold throughout Europe. This open market brought the price of wireless technology down, increased subscriber bases and, by adoption of a similar approach in the United States, ushered in today's ubiquitous smartphones and wireless networks.

Analogies can be drawn to current trends in blockchain standardisation. Blockchain is based on networks that are large enough – i.e. have enough nodes – to create reliability. As such, interoperability and scalability are important. Standardisation of blockchain elements can be an important tool in achieving those goals. But the standardisation process often involves competing visions. Certain companies will advance one approach, and other

companies will advance a different approach. That advocacy typically is based on a good faith belief, but it also arises from investments that companies make in their technology.

A meaningful standardisation process contains both risk and opportunity for our hypothetical company. No company wants to make the wrong bet and become the Betamax of blockchain technology. Companies therefore need to be thinking hard about the competing standards that are being created and what role they wish to play in that creation. An entirely passive role could result in other thought leaders seizing the marketplace, but too aggressive a role could lead to massive investments that are not adopted by the marketplace as a whole. Ultimately, every company needs to think about the role that they wish to play on that spectrum.

Acknowledgment

Jacob W.S. Schneider

The authors would like to thank Jacob Schneider, partner in Holland & Knight's Boston office, for his contribution to this chapter.

* * *

Endnotes

1. There are a range of other differences between public and permissioned networks as well. For example, a permissioned network can be structured with different consensus rules that reduce the resource requirements (including electricity requirements) needed on a public network such Bitcoin. There are also a range of gradations between fully public and fully private blockchain networks. The Enterprise Ethereum Alliance, for example, is designed to permit operation on a public network, but to restrict the nodes on that public network that receive the data at issue. *See* I. Allison, Enterprise Ethereum Alliance Is Back – And It's Got a Roadmap (May 2, 2018), located at https://www.coindesk.com/enterprise-ethereum-alliance-isnt-dead-got-roadmap-prove/.
2. Nakamoto, Satoshi, *Bitcoin: A Peer-to-Peer Electronic Cash System* (Oct. 31, 2008) (available at https://bitcoin.org/bitcoin.pdf).
3. 2008 is not the earliest disclosure of blockchain-like solutions. *See* Stuart Haber and W. Scott Stornetta (1991) and Bayer, Haber and Stornetta (1992).
4. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
5. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
6. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
7. https://blogs.thomsonreuters.com/answerson/in-rush-for-blockchain-patents-china-pulls-ahead.
8. http://patentvue.com/2018/01/12/blockchain-patent-filings-dominated-by-financial-services-industry.
9. https://www.ibm.com/blockchain.
10. https://www.delltechnologies.com/en-us/perspectives/tags/blockchain.
11. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).
12. Certain industry participants have been working to place restrictions on key patents, to prevent them from being acquired by NPEs. *See* Michael del Castilloite, Patent Trolls Beware: 40 Firms Join Fight Against Blockchain IP Abuse (March 16, 2017) located at

https://www.coindesk.com/40-blockchain-firms-unite-in-fight-against-patent-trolls/.

13. 35 U.S. Code § 154(a)(1) ("Every patent shall . . . grant to the patentee, his heirs or assigns, of the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States . . .").
14. https://blog.coinbase.com/how-we-think-about-patents-at-coinbase-26d82b68e7db.
15. *See* http://www.Bitcoin.org.
16. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing.
17. "About Hyperledger," located at https://www.hyperledger.org/about.
18. Enterprise Ethereum Alliance Specification Clears the Path to a Global Blockchain Ecosystem (May 16, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-specification-clears-path-global-blockchain-ecosystem/.
19. "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md; Downloads: DemoBench for Corda 3.0, located at https://www.corda.net/downloads/.
20. R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038.
21. Bitcoin software, for example, is licensed under the permissive, MIT Licence. *See* http://www.Bitcoin.org; https://opensource.org/licenses/MIT.
22. GPLv3 license, located at https://www.gnu.org/licenses/gpl-3.0.en.html.
23. L. Zeug, "Licensing" (September 4, 2016), located at https://github.com/ethereum/wiki/wiki/Licensing. *See, e.g.*, Ethereum-sandbox License, located at https://github.com/ether-camp/ethereum-sandbox/blob/master/LICENSE.txt.
24. Apache 2.0 license, located at https://www.apache.org/licenses/LICENSE-2.0.
25. For Corda, *see* R. Brown, "Corda: Open Source Community Update" (May 13, 2018) located at https://medium.com/corda/corda-open-source-community-update-f332386b4038; "Contributing to Corda," located at https://github.com/corda/corda/blob/master/CONTRIBUTING.md. For Hyperledger, *see* Brian Behlendorf, "Meet Hyperledger: An 'Umbrella' for Open Source Blockchain & Smart Contract Technologies" (September 13, 2016) located at https://www.hyperledger.org/blog/2016/09/13/meet-hyperledger-an-umbrella-for-open-source-blockchain-smart-contract-technologies. Code contributed to the Enterprise Ethereum Alliance is generally made available under an open source license that mirrors the Apache 2.0 license, *see* Enterprise Ethereum Alliance Inc. Intellectual Property Rights Policy, available at https://entethalliance.org/join/.
26. In defining the key term "based on", GPLv3 largely relies on copyright law rules governing derivative works. Courts generally rule that two copyrighted works are distinct (and one is not derivative of the other), if "they can live their own copyright life;" in other words, the test focuses on whether each expression "has an independent economic value and is, in itself, viable." *E.g., Columbia Pictures Indus. v. Krypton Broad. of Birmingham, Inc.*, 259 F.3d 1186, 1192 (9th Cir. 2001); *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, 964 F.2d 965, 969 (9th Cir. 1992).
27. For convenience, the code the developer is required to open-source in this manner is referred to as "Derivative Code".
28. GPLv3, sec. 11 (Patents).
29. GPLv3, sec. 10 (Automatic Licensing of Downstream Recipients).
30. The maintainer of the relevant Apache code at issue, through the Apache Software

Foundation, has the ability to set downstream terms for the contributed software.

31. Apache 2.0, sec. 3 (Grant of Patent License).
32. Our hypothetical company will also need to consider "compatibility" issues between various open source licences. The Hyperledger platform, for example, was unable to assimilate Ethereum code due to incompatibility between the Apache licence and strong copyleft licences, and the resulting need to obtain permissions from copyright owners to "re-license" the Ethereum code at issue. *See* J. Manning, Hyperledger Fails Ethereum Integration Due To Licensing Conflicts (February 3, 2017), located at https://www.ethnews.com/hyperledger-fails-ethereum-integration-due-to-licensing-conflicts; J. Buntinx, Ethereum app Developers may Face Licensing Issues Later on (December 6, 2017), located at https://www.newsbtc.com/2017/12/06/ethereum-app-developers-may-face-licensing-issues-later/.
33. IBM, for example, has contributed code under the Apache licence to the Hyperledger platform, and in turn is providing commercial Blockchain-as-a-Service (BaaS) offerings based on this platform using IBM's cloud infrastructure. *See IBM Blockchain, The Founder's Handbook: Your guide to getting started with Blockchain* (Edition 2.0) located at https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=28014128USEN. Microsoft has similar commercial offerings, based on Azure and the Enterprise Ethereum platform. *See* M. Finley, Getting Started with Ethereum using Azure Blockchain (January 24, 2018), located at https://blogs.msdn.microsoft.com/premier_developer/2018/01/24/getting-started-with-ethereum-using-azure-blockchain/.
34. A simple example is the shape and voltage of a wall power outlet. Because the power outlet is standardised among geographic regions, an appliance maker can ensure that its coffee maker will work (and can be sold) anywhere within a given region.
35. https://www.iso.org/committee/6266604.html.
36. http://standards.ieee.org/develop/project/2418.html.
37. http://standards.ieee.org/develop/project/825.html.
38. https://bita.studio.
39. https://www.hyperledger.org.
40. Enterprise Ethereum Alliance Advances Web 3.0 Era with Public Release of the Enterprise Ethereum Architecture Stack (May 2, 2018), located at https://entethalliance.org/enterprise-ethereum-alliance-advances-web-3-0-era-public-release-enterprise-ethereum-architecture-stack/; https://entethalliance.org/wp-content/uploads/2018/05/EEA-TS-0001-0-v1.00-EEA-Enterprise-Ethereum-Specification-R1.pdf.
41. Funk, Jeffrey L., Global Competition Between and Within Standards: The Case of Mobile Phones at 39 (New York, Palgrave, 2002); Garrard, Garry A., Cellular Communications: Worldwide Market Development (Boston, Artech House, 1998).
42. Gruber, Harald, The Economics of Mobile Telecommunications (Cambridge University Press, 2005) at 35.
43. *Id.*

Joshua Krumholz
Tel: +1 617 573 5820 / Email: Joshua.Krumholz@hklaw.com

Josh Krumholz is a partner in Holland & Knight's Boston office. A trial attorney and the national Practice Group Co-Leader for the firm's Intellectual Property Group, Mr Krumholz focuses primarily upon intellectual property litigation, with a particular focus on patent litigation. His practice covers a variety of technologies and jurisdictions. Mr Krumholz has successfully taken cases to jury verdict in the Eastern District of Texas, Illinois, Massachusetts, New York and New Jersey, among other jurisdictions. Technologies that Mr Krumholz handles include telecommunications, software, hardware, electronics and consumer goods. Mr Krumholz represents leading companies across a range of industries, including Ericsson Inc., T-Mobile, Inc., Verizon Corp., Avaya Inc., Acushnet Company and Hasbro, Inc., among others.

Ieuan G. Mahony
Tel: +1 617 573 5835 / Email: Ieuan.Mahony@hklaw.com

Ieuan Mahony is a partner in Holland & Knight's Boston office. He concentrates his practice in intellectual property (IP) licensing and development, data privacy and security, and information technology (IT). Mr Mahony combines his transactional and compliance work with dispute resolution and litigation matters. His substantial background in transactional and litigation practice areas helps clients receive high-quality advice in the dynamics of reaching an agreement as well as the realities of combating an adversary. Mr Mahony is a member of the firm's three-partner Information Technology Governance Committee.

Brian J. Colandreo
Tel: +1 617 305 2143 / Email: Brian.Colandreo@hklaw.com

Brian Colandreo is a partner in Holland & Knight's Boston office. Mr Colandreo serves as the National Patent Practice Leader and is a member of the Intellectual Property Group. A registered patent attorney, Mr Colandreo focuses his practice on client management, general intellectual property prosecution, transactional work, litigation support, due diligence work, and utility and design patent opinion work. Prior to entering law school, Mr Colandreo worked as a systems/software engineer for Johnson Controls.

Holland & Knight LLP

800 17th Street N.W., Suite 1100, Washington, DC 20006, USA
Tel: +1 202 955 3000 / Fax: +1 202 955 5564 / URL: www.hklaw.com

www.globallegalinsights.com

Other titles in the **Global Legal Insights** series include:

- **Banking Regulation**
- **Bribery & Corruption**
- **Cartels**
- **Corporate Tax**
- **Employment & Labour Law**
- **Energy**
- **Fund Finance**
- **Initial Public Offerings**
- **International Arbitration**
- **Litigation & Dispute Resolution**
- **Merger Control**
- **Mergers & Acquisitions**
- **Pricing & Reimbursement**

Published by: glg global legal group

Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

The Regulatory Concerns Of Crypto Exchange Registration

By **Jennifer Connors, Josias Dewey, Rebecca Leon and David Sofge** (May 3, 2018, 2:40 PM EDT)

Jennifer Connors

Josias Dewey

Coinbase, one of the largest cryptocurrency exchanges, recently approached the U.S. Securities and Exchange Commission about possible licensing as a broker-dealer. If Coinbase decides to register, it will become among the first of the existing cryptocurrency exchanges to be registered with the SEC. This news comes on the heels of a pronouncement by the SEC Division of Trading and Markets, warning that platforms that offer or trade digital assets that are deemed to be securities, including many initial coin offerings, must register as a national securities exchange or otherwise be exempt from such registration.

In consideration of these recent events and pronouncements, other digital asset exchanges should take note of the regulatory concerns and exemptions related to their operations. While it appears that Coinbase's determination is related to its intention to broaden its offering beyond traditional cryptocurrency, the SEC's statement regarding the trading of digital assets leaves little doubt that, in its view, most ICOs will constitute a securities offering. This article provides a brief overview of the registration options available to digital asset platforms and the benefits and restrictions of registration as a national securities exchange, a broker-dealer operating an alternative trading system, or a funding portal.

National Securities Exchange Registration

The SEC's statement concludes that an online trading platform that brings together buyers and sellers of digital assets deemed to be securities would need to be registered with the SEC as a national securities exchange under Section 6 of the Exchange Act, unless it is otherwise exempt from such registration.

The process of registering as a securities exchange is complex, time-consuming and subject to the SEC's determination that such entity is able to comply with all requirements imposed on exchanges, such as enforcing compliance by its members with its rules as well as the federal securities laws. Fundamentally, registered national securities exchanges are self-regulatory organizations and as such (subject to SEC oversight and approval under Section 19(b) of the Exchange Act), an exchange is able to establish its own rules regarding trading, conduct of members, and applicable fees. Additionally, an exchange is responsible for the supervision and compliance of its members with applicable regulations and therefore has an obligation to develop and maintain inspection and disciplinary programs, as well as monitor and conduct appropriate surveillance of the activities of its members. Under the Exchange Act, a national securities exchange must provide fair access to its members. Although it may limit membership through reasonable standards for access, such standards must not be discriminatory. Finally, all members of a national securities exchange must be registered broker-dealers or persons associated with a

registered broker-dealer.

Rebecca Leon

Takeaway: While the foregoing obligations are no doubt significant and onerous, certain business models may favor the application of a national securities exchange model. If a digital asset exchange wishes to register with the SEC as a national securities exchange, it may enjoy its status as an SRO, which allows it to set its own rules and dictate how it wishes to operate. Certain exchanges may find that control over listing fees from issuers will allow an exchange to better sustain its business model. In addition, while an exchange has significant monitoring and supervisory responsibilities relating to its members, increasingly, SROs contract out a significant portion of their regulatory obligations through a regulatory services agreement. Importantly, the exchange would be limited to admitting members who are registered broker-dealers or their associated persons, thus impeding the ability for retail customers or issuers to trade without the use of an intermediary.

Alternative Trading System Registration

David Sofge

Another option for a cryptocurrency exchange is Regulation ATS, which exempts an ATS from registering as a national securities exchange if it registers as a broker-dealer and provides the SEC with certain information regarding its operations on Form ATS. An ATS generally receives and executes orders in securities electronically through its trading system. While exempt from registration as a national securities exchange, a firm relying on Reg ATS (known as a sponsor) remains subject to several regulatory requirements, some of which are required by Reg ATS, and some of which are due to its status as a broker-dealer.

An ATS also has several ongoing reporting requirements. As with registered national securities exchanges, an ATS may be required to provide fair access to the trading system (provided that trading on the ATS reaches certain thresholds). Additionally, the ATS must establish adequate safeguards and procedures to protect subscribers' confidential trading information and make and maintain prescribed books and records. In order to prevent customer and market participant confusion, an ATS is prohibited from using "exchange," or derivations such as the term "stock market," in its name.

In addition to Reg ATS, additional issues may arise from the ATS' registration as a broker-dealer and compliance with all applicable SEC and Financial Industry Regulatory Authority rules under broker-dealer regulation, including, but not limited to:

- ***Customer Protection:*** Under SEC Rule 15c3-3, a broker-dealer must maintain the physical possession or control of all fully paid securities and excess margin securities carried by the broker-dealer for the account of its customers. A common feature underlying cryptocurrency or digital asset exchanges is the use of distributed ledger technology whereby transactions are recorded on a database that is maintained over a public or private network. Broker-dealers need to consider how the use of DLT impacts the receipt, delivery and custody of securities and other assets of their customer's accounts. For example, will ICO tokens, securities or other assets be held in an individual's account (wallet) or will the sponsor of the ATS provide for the custody of these securities and assets with a third-party qualified custodian?

- ***Books and Records:*** Registered broker-dealers must make and maintain current books and records. Specifically, Rules 17a-3 and 17a-4 under the Exchange Act and FINRA Rule 4511 require that broker-dealers preserve certain records for specified periods of time. The use of DLT must be considered as it potentially impacts a broker-dealer's requirements under these rules. For example, certain records must be maintained for a period of time in a prescribed manner (i.e., solely electronic records must be stored in a "write once read many," or WORM, format). How will a digital-asset ATS ensure that the DLT is recording and maintaining such

information in compliance with applicable rules?

- ***Fees:*** To the extent that a subscriber participating on a digital-asset ATS would be subject to any fees or commissions, additional concerns may arise. Regulatory requirements may apply if a subscriber is subject to fees for the management of wallets and keys, onboarding, or commissions or markups for trades placed through the ATS.

- ***Examinations:*** Dangers relating to regulatory examinations may also arise. Potential registrants and regulators are still in the nascent stages of understanding these new technologies and how existing regulations apply. FINRA's current examination module for an ATS may very well be largely inapplicable to a cryptocurrency or digital-asset ATS.

Takeaway: If a cryptocurrency exchange registers as an ATS, it may have less stringent regulatory requirements than it would if it registers as a national securities exchange. However, the cryptocurrency ATS must still consider the regulatory impact of registration as a broker-dealer.

Funding Portal Registration

The Jobs Act exempts certain intermediaries that operate "funding portals" from the requirement to register with the SEC as a broker-dealer. A funding portal is defined as a crowdfunding intermediary that does not (1) offer investment advice or recommendations, (2) solicit purchases, sales or offers to buy the securities offered or displayed on its website or portal, (3) compensate employees, agents or other persons for such solicitation or based on the sale of securities displayed or referenced on its website or portal, (4) hold, manage, possess or otherwise handle investor funds or securities, or (5) engage in such other activities as the commission, by rule, determines appropriate.

A registered funding portal must be a member of FINRA. While the funding portal does not need to register as a broker-dealer, it remains subject to FINRA's and the SEC's examination, enforcement and rulemaking authority. A funding portal is required to, among other things, provide disclosures and investor education materials to investors, take steps to protect the privacy of information collected from investors, and make efforts to ensure that no investor in a 12-month period has purchased crowdfunded securities that, in the aggregate, from all issuers, exceed certain investment limits.

Takeaway: The crowdfunding portal option is clearly the most limited option for a potential registrant. The activity would be limited to the relatively passive listing of ICOs. Moreover, the compensation model for an operator is limited as well as the receipt of transaction-based compensation is prohibited. Nevertheless, this may be an option depending on the business model and potential issuer base of the digital currency platform.

Conclusion

If Coinbase completes this regulatory process and becomes an SEC-registered exchange, it may herald a wave of registration with the SEC. In this event, these exchanges should take note of the regulatory requirements and concerns related to such registration to decide which option fits best with their current and proposed business model.

Jennifer A. Connors is a partner in the New York office of Holland & Knight LLP.

Josias N. Dewey and Rebecca Leon are partners in the firm's Miami office.

David P. Sofge is an attorney in Holland & Knight's Fort Lauderdale, Florida, office.

Holland & Knight

ALERT

Offering Exemptions Available to Companies Issuing ICOs

May 14, 2018

Jennifer A. Connors
Josias N Dewey
Rebecca Leon
David P Sofge

Qualifying for the race

HIGHLIGHTS:

- Issuing an initial coin offering (ICO) is a new and innovative way for companies to infuse capital into their enterprise. However, several regulatory agencies have increased their scrutiny of ICOs, including the U.S. Securities and Exchange Commission (SEC).
- While ICOs represent an exciting new possibility for capital raises, much uncertainty remains with respect to ongoing regulation and therefore compliance with applicable securities laws is needed to ensure a smooth offering. Failure to comply with applicable securities registration and offering requirements can have severe consequences for the issuer and those involved in the offering and may provide investors with a right of rescission.
- This client alert provides a high-level overview of certain offering exemptions available to a company intending to conduct an ICO pursuant to Regulation D, Regulation A-Plus, Regulation CF or Regulation S.

Issuing an initial coin offering (ICO) is a new and innovative way for companies to infuse capital into their enterprise. One survey recently estimated that the average ICO issued in 2017 raised $12.7 million for each issuing company and current data indicates that ICOs issued in 2018 have already surpassed the total amount of funds raised last year. However, several regulatory agencies have increased their scrutiny of ICOs, including the U.S. Securities and Exchange Commission (SEC). According to recent statements by the SEC, most "tokens" or "coins" issued through an ICO are securities and companies issuing ICOs must consider how these offerings implicate the securities

registration requirements of the federal securities laws.

Companies may find relief from the securities registration requirements through one or more of the exempt offering options provided under federal securities laws. This client alert provides a high-level overview of certain offering exemptions available to a company intending to conduct an ICO pursuant to Regulation D, Regulation A-Plus, Regulation CF or Regulation S.

Exemption	Pros	Cons
Reg D 506(b)	• No capital fundraising limit • Relatively limited filing requirements	• **Cannot** solicit/advertise to the public • Generally must limit to accredited investors (self-certified); 35 nonaccredited • Resale limitations • State law requirements
Reg D 506(c)	• No capital fundraising limit • Relatively limited filing requirements	• **Can** solicit/advertise to the public • Must limit to only accredited investors (reasonably verified) • Resale limitations • State law requirements
Reg A-Plus (Tier 1)	• $20 million capital fundraising limit in a 12-month period • No limits on type of investors (can be offered to general public) • No limits on resale	• Qualification by the SEC and the respective states required
Reg A-Plus (Tier 2)	• $50 million capital fundraising limit in a 12-month period • No limits on type of investors (can be offered to general public) • Initial offering exempt from state registration	• SEC qualification only • Ongoing disclosure requirements • State qualification may be required for resales
Reg CF	• No limits on type of investors (can be offered to general public)	• Low capital fundraising limit and limited amount per investor • Increased reporting

		obligations • Resale limitations
Reg S	• No capital fundraising limit	• Increased monitoring to ensure all investors are non-U.S. persons • May be subject to restriction and registration in foreign jurisdictions • Resale limitations

Regulation D

Regulation D provides for two exemptions under Rule 506(b) and Rule 506(c).

Under Rule 506(b), a company conducting an ICO is not subject to any limitation on the amount of money it can raise pursuant to this offering exemption. However, a company may not use general solicitation or advertising to market the offering and must generally limit its sales to financially sophisticated or accredited investors (or up to 35 nonaccredited investors, provided such investors receive certain additional disclosures). Because of the prohibition on solicitation, the company must generally know that such investors are qualified as accredited investors and may rely on the investors' certification of their status to do so.

Under Rule 506(c), a company conducting an ICO is also not subject to any limitations on the amount of money it can raise. Moreover, under this exemption, a company is permitted to broadly solicit and advertise the ICO, provided that all of the investors are accredited investors. Accordingly, the company may not rely solely on such investors' representations, but must take reasonable steps to verify their status as such.

Both Rule 506(b) and Rule 506(c) require companies to file a notice on Form D that includes the names of the company's executive officers and directors and some limited information about the offering. State regulators also have Form D filing requirements. Finally, under both rules, the tokens or coins issued through the ICO would be restricted securities, which cannot be freely resold in a public marketplace for six months or a year.

Takeaway: A Regulation D exempt offering may be enticing for companies planning on issuing an ICO as it affords no limitation on the amount of capital that may be raised and the regulatory filing requirements are relatively minimal. However, companies that are contemplating an ICO through this exemption are limited by the type of investors who may invest in such offering. To this point, the company should consider the feasibility of sourcing sufficient accredited investors as well as the operational burden of ensuring that investors are accredited and adhering to limitations applicable to nonaccredited investors.

Regulation A-Plus

Like Regulation D, a Regulation A (now known as Regulation A-Plus because of the amendments promulgated by the JOBS Act in 2015) may be available through two options. These options are generally available to U.S. or Canadian issuers not currently subject to reporting requirements of the federal securities laws or subject to a "bad actor" disqualification. In both cases, the offering may be made to the general public and, unlike Regulation D, the coins or tokens so issued are not restricted securities.

The first option, a Tier 1 offering, allows a company to raise up to $20 million in any 12-month period. A company conducting an ICO under this exemption must provide investors with an offering circular which must be filed with, and is subject to review and qualification by, the SEC as well as state regulators where the ICO is being conducted. The offering circular should include information about the ICO, describe the use of proceeds and the risks of the ICO and describe selling shareholders, the company's business, management, performance, plans and financial statements. However, after the offering circular has been filed with the SEC and any applicable state regulators, the company has no other ongoing reporting obligations.

The second option, a Tier 2 offering, allows a company to raise up to $50 million in any 12-month period. Like Tier 1 offerings, companies must give investors access to an offering circular and file with the SEC for review and qualification. However, the company does not need to file with any state securities regulator. Unlike Tier 1 offerings, companies offering under Tier 2 are subject to ongoing reporting requirements and must regularly disclose their financial results and file reports with the SEC. Moreover, Tier 2 limits how much individual investors can invest depending on such investors' net worth, which they may self-certify, provided the company has no knowledge that an investor has exceeded such limit. Additionally, while tokens or coins issued under either tier of Regulation A-Plus are not restricted securities, qualification by state regulators (Blue Sky Laws) may be required for secondary trades in Tier 2 issues.

Takeaway: Regulation A-Plus may be attractive for smaller companies issuing an ICO that are looking to raise capital through the offering of tokens or coins while avoiding some of the more burdensome disclosure requirements. Companies can raise a large amount of capital and, unlike under Regulation D, are not limited to certain types of investors. While a company issuing an ICO under this exemption has some initial (and potentially ongoing) reporting obligations, these requirements are not as burdensome as they would be under a public offering regime.

Regulation CF

Under Regulation CF, a company can raise $1.07 million over a 12-month period. Certain companies are not eligible to use this offering exemption, such as non-U.S. companies, Exchange Act reporting companies, certain investment companies and others. Further, Regulation CF limits how much individuals can invest depending on their net worth. The entire Regulation CF offering must be conducted through an online intermediary registered with the SEC as a funding portal or broker-dealer. The company may not advertise the terms of the offering, except in a limited notice directing potential investors to the registered online intermediary. However, the company can, through the registered online intermediary, communicate with investors regarding the terms of the ICO. Finally, tokens or coins issued in an ICO cannot be resold in public markets within a one-year period.

A company conducting a Regulation CF offering must file an Offering Statement Disclosure via Form C with the SEC, which discloses certain information about the company and its business. Furthermore, a company that offers securities through Regulation CF has a continued reporting obligation and must provide an annual report that contains certain information about the company.

Takeaway: Regulation CF provides for the lowest capital amount and imposes heightened reporting obligations on a company issuing an ICO. Furthermore, while there are no restrictions on the type of investors, these investors are more limited in how much they can invest compared to the limits established in Regulation A-Plus.Nevertheless, this exemption does provide a fundraising avenue to many small companies that may have previously turned exclusively to friends and family or utilized bank loans.

Regulation S

Another potential avenue for companies is to engage in a purely offshore offering to non-U.S. persons pursuant to Regulation S. It should be noted however, that companies relying upon this offering exemption must take several steps to ensure that potential investors are indeed non-U.S. persons and take steps to ensure that securities are not offered into the U.S. without registration. Moreover, companies need to be aware of the offering restrictions and registration requirements of the various countries in which their investors reside, thus creating a complex task for an issuer seeking to take advantage of this exemption. In addition, similar to the other offering exemptions, resales using the public markets in the U.S. are not permitted unless a seller uses another applicable offering exemption.

Takeaway: In addition to enforcing restrictions on sales to U.S. persons, a company seeking to conduct an ICO through Regulation S must ensure that it is knowledgeable about the offering restrictions in the countries in which non-U.S. investors reside to avoid adverse regulatory action and/or rescission by such investors.

Conclusion

While ICOs represent an exciting new possibility for capital raises, much uncertainty remains with respect to ongoing regulation and therefore compliance with applicable securities laws is needed to ensure a smooth offering. Depending on a company's goals and tolerance for associated regulatory burdens, the company may have a strong preference for a certain form of exempt offering. These offering exemptions provide a "middle ground" for a company looking to raise capital when compared to other capital raising initiatives, such as offerings to private equity firms, venture capital firms and public offerings under the federal securities laws.

Clients with questions regarding exemptions for companies issuing ICOs, may contact Jennifer Connors, Josias Dewey, Rebecca Leon or David Sofge.

Authors

Jennifer Connors is a New York financial services attorney who represents broker-dealers, alternative trading systems (ATSs), financial technology (FinTech) companies and other market participants on securities law and market regulation matters. Ms. Connors' practice has a particular emphasis on broker-dealer regulation and compliance issues, trading rules, issues regarding ATSs, electronic trading, cybersecurity, sales practices and anti-money laundering (AML) rules. She also advises FinTech companies and fund management clients with respect to broker-dealer regulation issues, as well as securities offerings and private placements.
212.513.3443 | Jennifer.Connors@hklaw.com

Josias "Joe" N. Dewey is a financial services and real estate attorney and is considered a thought leader on blockchain and distributed ledger technology (DLT). Mr. Dewey is the co-author of the book, "The Blockchain: A Guide for Legal and Business Professionals," published by Thomson Reuters. Mr. Dewey formally served as the leader of Holland & Knight's Miami Real Estate practice group.
305.789.7746 | joe.dewey@hklaw.com

Rebecca Leon is a financial services regulatory attorney in Holland & Knight's Miami office, and a member of the firm's Financial Services Team. Ms. Leon advises broker-dealers, investment advisers, fund managers, banks and other wealth managers on a variety of U.S. and international regulatory and operational matters.
305.789.7703 | Rebecca.Leon@hklaw.com

David Sofge is an attorney in Holland & Knight's Fort Lauderdale office. He represents public and private companies in corporate and financing transactions and regulatory compliance.
954.468.7884 | David.Sofge@hklaw.com

What IP Practitioners Should Know About Blockchain

Joshua Krumholz

April 5, 2019

Holland & Knight

#57876739

Summary of Topics

- Patenting Blockchain Concepts
- The Role and Impact of Open Source Software
- The Threat of Litigation
- Lessons from Telecom Standards

Patenting Blockchain Concepts – Blockchain Basics Are Not Patentable

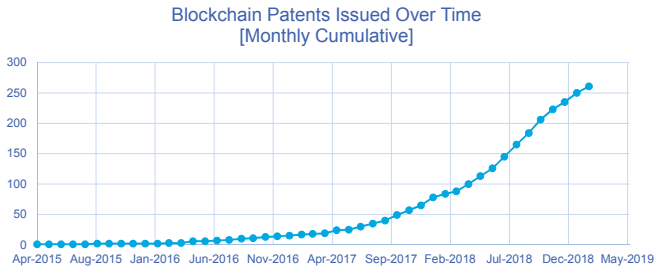
- The creator of blockchain, under the pseudonym Satoshi Nakamota, dedicated his basic concepts to the public in 2008, making them unpatentable
- Many blockchain concepts are unpatentable abstract ideas under *Alice*
- The absence of foundational patents may have sped up development
- Ideas implementing blockchain technology can be patentable

Patenting Blockchain Concepts – Many Potential Applications

- There are a large number of potential applications that could lead to patentable ideas
- Examples include the HSBC's new blockchain platform, JP Morgan's JP Coin, the Boomerang Project, Tari Tickets and the Codex Project
- Challenges that could be overcome by blockchain include –
  - Safely and securely transferring medical records
  - Addressing counterfeit drugs
  - Tracking food from farm to table

Patenting Blockchain Concepts – Applications and Allowed Patents

- The PTO has allowed over 260 blockchain-related patents, up from 2 in 2015 to 170 in 2018
- Over 1,500 patent applications are pending
- Chinese companies account for a significant number of applications



Patenting Blockchain Concepts – Examples of Allowed Patents

- U.S. Patent No. 10,055,446 – Ensuring Data Integrity of Executed Transactions
- U.S. Patent No. 9,875,510 – Consensus System for Tracking Peer-to-Peer Digital Records
- U.S. Patent No. 9,807,106 – Mitigating Blockchain Attacks

The Role and Impact of Open Source Software

- Open source software – Software that is distributed in source code form and available for use by anyone to test, modify and use. Open source source code is unrestricted
- Proprietary software – Software that is distributed in object code only. The source code is protected as a trade secret, and cannot be modified without permission of the developer

The Role and Impact of Open Source Software – Public and Permissioned Networks

- Public networks (Ethereum, Bitcoin) – Nodes are anonymous and each node contains all transactions
- Permissioned networks (Enterprise Ethereum, Hyperledger, Corda) – Network members are vetted and approved, the nodes are not anonymous, and transactional information can be selectively disclosed
- Business networks typically are permissioned networks, and that is especially the case for businesses that are regulated, like financial institutions

The Role and Impact of Open Source Software – Networks Use Open Source Software

- Blockchain networks are based on open source software
- The General Public License, version 3 ("GPLv3") governs large portions of the Ethereum code base
- The Apache 2.0 license ("Apache") governs open source software used for Hyperledger, Corda and Enterprise Ethereum
- The rights and duties of the users of the above networks may be substantially impacted by these open source licenses

The Role and Impact of Open Source Software – GPLv3 and Apache Terms

- GPLv3 license (Ethereum)
  - Strong "copyleft" license
  - If a developer incorporates GPLv3 code into his/her proprietary code, the developer must make that proprietary code publicly available and royalty-free, including a royalty-free license for patents that cover the code (to the extent necessary to use the code)
- Apache license (Hyperledger, Corda and Enterprise Etherium)
  - Apache is more flexible that GPLv3
  - Using the software is not enough to restrict rights; the developer needs to affirmatively contribute the proprietary code to the network for restrictions to apply
  - The restrictions are similar to GPLv3, except that the developer can sue for patent infringement, but then loses the right to use the Apache code

The Role and Impact of Open Source Software – Making Conscious Choices

- The foregoing would suggest that developers stay away from Hyperledger, but in fact IBM and Microsoft have made significant contributions to that code base
- The important lesson is to make sure that developers are not choosing the code base to use without input from legal, otherwise they may be unintentionally giving away the company's IP rights

The Threat of Litigation Generally

- As a highly disruptive technology, blockchain has the potential of drawing significant litigation
- Examples include:
  - Fraud cases, which presently are the vast majority of cases
  - Litigation brought by threatened stakeholders
  - Litigation brought by blockchain partners
- Blockchain implementers need to consider carefully
  - The impact of the change on stakeholders and whether any exposure exists
  - The terms and agreements they have with their blockchain partners

The Threat of Patent Litigation – Blockchain as a Potential New Wave of Litigation

- In recent years, the threat of patent litigation has waned due to changes in the law and the market
- Blockchain may cause an increase of patent litigation because:
  - A competitive landscape may cause companies to use their patents as a sword
  - There are many new patents that have not yet been licensed
  - Blockchain technology is being used in lucrative fields
  - Blockchain technology will likely be used as fundamental building blocks
- Trolls are already getting themselves ready
  - And failed startups may become trolls down the line

The Threat of Patent Litigation – Pre-Litigation Strategies

- Cross-licensing. The companies with the largest portfolios will cross-license with each other
- Patent pools. License-based organizations that accumulate patents to take them off the market are already being formed in this field
- Monitoring patent applications and issuances. Monitoring is doable given the volume but may come with some risk of establishing willfulness
- Design-arounds. It is easier to avoid a patent during the design phase than to try to change the product after launch
- IPRs. *Inter Partes* Reviews can be filed before litigation

The Threat of Patent Litigation – Strategies Once You Are in Litigation

- IPRs. IPRs can be filed up to one year from the filing of the lawsuit
- Open source defenses. Open source restrictions follow a patent after transfer, so should be considered in any defense strategy
- Attacking on *Alice* grounds. Concept patents should not be allowed, but sometimes they are and are vulnerable to attack
- Asserting counterclaims. You need to assess the extent to which you can use your portfolio to assert patent infringement against the plaintiff

The Threat of Patent Litigation – Patent Pledges

- Unilateral patent pledges – Coinbase and Blockstream have pledged to use blockchain patents only for defensive purposes
- Multilateral patent pledges – Members of an organization agree not to sue each other. Examples include DPL, LoT and OIN
- Challenging approach and done by companies that probably would cross-license anyway

Lessons From Telecom Standards – Creating Blockchain Standards

- Standards could help with blockchain scalability
- Standards efforts are already underway
  - Blockchain in Transportation Alliance (BiTA)
  - International Standards Organization (ISO)
  - Institute of Electrical and Electronics Engineers (IEEE)
- To participate or not to participate in standards creation
  - Pros: Helping to shape the future, staying up to date on developments, avoiding being the Betamax of blockchain
  - Cons: It is a major investment and commitment, and you still may end up as the Betamax of blockchain

Lessons from Telecom Standards – Challenges

- Because blockchain potentially covers so many industries, it may be hard to get consensus on what technology to standardize
- Standards lead to standard-essential patents, which can exacerbate patent litigation threats
- Establishing FRAND (fair, reasonable and nondiscriminatory) terms with so many different industries could be challenging

Ethical Considerations in Information Gathering and Evolving Technologies.

William Belmont
The Belmont Group, LLC

Pery D. Krinsky
Krinsky PLLC

Cornell Journal of Law and Public Policy

Volume 24 | Issue 1 Article 4

Neither Friend nor Follower: Ethical Boundaries on the Lawyer's Use of Social Media

Robert Keeling

Tami Weerasingha-Cote

John Paul Schnapper-Casteras

NEITHER FRIEND NOR FOLLOWER: ETHICAL BOUNDARIES ON THE LAWYER'S USE OF SOCIAL MEDIA

*Robert Keeling, Tami Weerasingha-Cote & John Paul Schnapper-Casteras**

A handful of state and local bars have begun to opine on lawyers' use of social media in conducting investigations and informal discovery. Despite the increasing prevalence and diversity of social media, however, these few bar authorities have addressed lawyers' use of social media in ways that are formalistic, limited in their technical explanations and analogies, and even, at times, arbitrary. As a result, the use of social media by litigants and their counsel has been needlessly and baselessly deterred. Rather than trying to address social media by relying on inapposite analogies to the "real world" and grasping at some transient definition of what is "public" vs. "private" information, state and local bars should focus their analyses on the application of the existing Rules of Professional Conduct and the time-tested prohibitions on fraud and deception. Further, the ABA, state bars, and other committees seeking to address the unique ethical questions and challenges raised by lawyers' use of social media information should engage in a careful and informed study of the nature and functionality of social media as a new and distinct method of producing and sharing information before seeking to constrain its use under the existing Rules of Professional Conduct.

* Robert D. Keeling is a partner at Sidley Austin LLP whose practice includes a special focus on electronic discovery matters. Tami Weerasingha-Cote is an associate at Sidley Austin LLP. JP Schnapper-Casteras is at attorney at the NAACP Legal Defense Fund. This Article reflects the views of the authors alone and does not necessarily reflect the opinions of their respective current or former employers.

INTRODUCTION

Under the smattering of ethics opinions and secondary guidance that currently exist, intuitive and common uses of popular social media sites by lawyers seeking information through informal discovery are either prohibited or considered ethically questionable enough so as to chill their use. For example, one local bar association has concluded that lawyers may not seek access to non-public information posted by other litigants on Facebook, either because the automatically generated "friend" request message is an ethically impermissible "communication" with a represented party, or because such a message does not explicitly disclose the motives of the request to an unrepresented party.[1] Following this logic, the act of clicking the "follow" button on another party's Twitter page, which normally generates an automatic email notification, could also be ethically impermissible, even though millions of people "follow" public figures and friends on Twitter. Viewing the resumes of friends and strangers alike on a site like LinkedIn is a widely accepted practice in professional circles, yet if a lawyer views a litigant's page, that too generates a notification message which could conceivably constitute an impermissible "communication."

The few ethics opinions addressing the use of social media in informal discovery have focused largely on Facebook and MySpace, and most do not directly address limits on using Twitter, LinkedIn, and other social media platforms. Some practitioners, however, have read these opinions to limit informal discovery of social media information more broadly to public information only.[2] Given the serious consequences of

---

[1] San Diego Cnty. Bar Legal Ethics Comm., Op. 2011–2 (2011), *available at* https://www.sdcba.org/index.cfm?pg=LEC2011-2.

[2] *See, e.g.*, PRACTICING LAW INST., SOCIAL MEDIA AND THE LAW § 9:6.2 (Kathryn L. Ossian ed., 2013); Andy Radhakant & Matthew Diskin, *How Social Media Are Transforming Litigation*, LITIG., Spring 2013, at 17.

violating ethical boundaries, this caution is understandable. Despite these concerns, the fact remains that such limitations are overbroad and unworkable.

In the physical world, lawyers routinely seek information about other parties and witnesses outside of formal discovery procedures in order to get a full understanding of the facts, develop appropriate litigation strategies, and craft effective discovery requests. For example, lawyers frequently conduct public record searches and utilize private investigators in order to obtain facts not publicly available. Indeed, courts have recognized the critical importance of such informal discovery in the expeditious processing and resolution of cases.[3] Generally, the rules of professional conduct limit such informal discovery only to the extent that the rules prohibit deceptive and fraudulent conduct, as well as inappropriate communications with represented persons. In the realm of social media, lawyers should be able to seek information just as freely. To the extent several state and local bars seek to limit informal discovery of social media content by likening the use of social media applications to "real-world" communications, this reasoning often reflects a poor understanding of how such applications work, and fails to account for the immense diversity in social application types and functionality. To the extent practitioners are attempting to create clear rules of conduct for social media research by reading existing ethics opinions as creating a bright-line distinction between "public" and "non-public" social media content, such a distinction is vague and impracticable, and will only prove more so as technology develops over time.

Instead of grasping for some hazy definition of what is "public" or trying to force social media usage into the mold of "real-world" communication, bar ethics committees and drafters of model rules should embrace standards that acknowledge the unique nature of social media information. Specifically, we suggest that the use of social media in informal discovery be governed by longstanding principles that censure deception and fraud and we urge a commonsense understanding of what types of virtual contact actually constitute "communication" under the rules of professional conduct. Such standards will better serve plaintiffs, defendants, and judicial administration because they would facilitate the exchange of information, the basis of well-founded formal discovery, and the efficient resolution of cases. Ultimately, rather than fragment and foreclose the social media landscape from informal discovery, the

---

[3] *See, e.g.*, Niesig v. Team I, 558 N.E.2d 1030, 1034, 76 N.Y.2d 363, 372 (N.Y. 1990) (describing informal discovery as serving both the litigants and the entire justice system by uncovering relevant facts, thus promoting the expeditious resolution of disputes); Muriel Siebert & Co. v. Intuit Inc., 868 N.E.2d 208, 210, 8 N.Y.3d 506, 511 (N.Y. 2007) (explaining that informal discovery could streamline discovery and foster the prompt resolution of claims).

governing principles should reflect the reality that social media is here to stay. Social media contains increasingly voluminous and relevant information for litigation, and should be usable by litigants within reasonable ethical bounds.

To this end, Part I of this Article details sources of authority and interpretations of the prevailing view that informal discovery of social media information is limited to that which is publicly available. Part II lays out and provides support for our view that, in fact, such discovery is broadly permissible under traditional rules of professional conduct.

I. PREVAILING VIEW: INFORMAL DISCOVERY OF SOCIAL MEDIA ACCOUNTS IS LIMITED TO INFORMATION THAT IS PUBLICLY AVAILABLE

The most authoritative bodies on the ethical obligations of practicing lawyers—the American Bar Association (ABA) and several state bar associations—have provided very little guidance on how lawyers may permissibly seek information from social media sites through informal discovery. Currently, neither the ABA's model rules of professional conduct nor any state version of these rules explicitly addresses social media in any way. A handful of state and local bar ethical opinions applying existing rules to various social media research scenarios provide a few dots on the map, but the only consistent conclusion these few opinions share is that publicly available information is fair game. Practitioners have naturally clung to this rule—that informal discovery of social media accounts is limited to information that is publicly available—as the only clearly demarcated boundary line, and have propagated it accordingly.

A. State and Local Bars

The Model Rules of Professional Conduct and their commentaries do not explicitly address the permissibility of informal discovery of social media information. Several state and local bars, however, have issued ethics opinions that address one or more aspects of this complex issue. Although each opinion applies the relevant rules of professional conduct to different and highly specific factual scenarios, several analytical themes are common to the group of opinions as a whole.

In 2005, the Oregon State Bar issued one of the first bar association opinions on the subject of informal discovery of social media. The opinion addresses whether a lawyer, in anticipation of litigation, may visit the website of a represented party, and whether the lawyer may "communi-

cate via the Web site" with representatives of that party.[4] The opinion identifies the prohibition on a lawyer from communicating with another party known to be represented about the subject of the representation as the applicable rule,[5] noting that "the purpose of the rule is to ensure that represented persons have the benefit of their lawyer's counsel when discussing the subject of the representation with the adverse lawyer."[6] The opinion also takes as its premise that "there is no reason to distinguish between electronic or nonelectronic forms of contact. Both are permitted or both are prohibited."[7] Reasoning that accessing an adverse party's public website is "no different from reading a magazine article or purchasing a book written by that adversary," the opinion concludes that such activities are permissible because "the risks that [the relevant rule] seeks to avoid are not implicated by such activities."[8] As to whether the lawyer may "communicate via the Web site" with representatives of the adverse party, the opinion states that the relevant distinction is whether the individual with whom the lawyer wants to communicate is a "represented person" within the meaning of the rules of professional conduct.[9] The opinion does not specify what type of activity via a website is considered "communication," but concludes that, just as with any other written communications, if the individual contacted is a represented person (e.g., a managerial employee of the adverse party), then the communication is prohibited, but if the individual is a "nonmanagerial employee who is merely a fact witness," then such communication is permissible.[10]

In 2009, the Philadelphia Bar Association Professional Guidance Committee tackled the question of whether an ethical violation occurs if a lawyer, seeking access to the non-public content of a witness's Facebook and MySpace accounts, asks a third person (someone whose name the witness will not recognize) to "friend" the witness and seek

---

4 Or. Bar Ass'n, Formal Op. 2005-164 (2005), *available at* http://www.osbar.org/_docs/ethics/2005-164.pdf.

5 *Id.* Oregon Rule of Professional Conduct 4.2 provides: "In representing a client or the lawyer's own interests, a lawyer shall not communicate or cause another to communicate on the subject of the representation with a person the lawyer knows to be represented by a lawyer on that subject unless: (a) the lawyer has the prior consent of a lawyer representing such other person; (b) the lawyer is authorized by law or by court order to do so; or (c) a written agreement requires a written notice or demand to be sent to such other person, in which case a copy of such notice or demand shall also be sent to such other person's lawyer." OR. RULES OF PROF'L CONDUCT R. 4.2 (2014). This rule is very similar to Rule 4.2 of the American Bar Association (ABA) Model Rules of Professional Conduct, except that the Model Rule does not apply to lawyers acting in their own interest, and it makes no exception for communications required by written agreements. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2013).

6 Or. Bar Ass'n, *supra* note 4.

7 *Id.*

8 *Id.*

9 *Id.*

10 *Id.*

access to this information.[11] In this scenario, the witness was neither a party to the litigation nor represented, and the third person stated only truthful information in the request for access, but did not disclose her relationship with the lawyer.[12] The opinion identifies two rules as relevant to its inquiry: (1) the rule holding lawyers responsible for the conduct of their nonlawyer assistants, and (2) the rule stating that it is professional misconduct for a lawyer to engage in acts involving dishonesty, fraud, deceit, or misrepresentation.[13] Noting that the lawyer would be responsible for the actions of the third person under the first rule, the opinion determines that the proposed course of action would be unethical under the second rule.[14] Although the third person intends to use only truthful information in the request for access, the opinion concludes that the request would still be "deceptive" because it does not disclose the true purpose of the request––gaining access to information that will be shared with, and may be used by, the lawyer in litigation.[15] Recognizing that individuals often grant access to their social media content without knowing the motivations of those seeking access to it, the opinion nonetheless concludes that any deception on the part of other social media users does not change the fact that such deception at the direction of a lawyer is a violation of ethical rules.[16] Interestingly, the opinion explicitly permits the lawyer to ask the witness "forthrightly" for access, although it is not clear whether such a request must include an explicit disclosure that the information is sought for the purposes of litigation, or whether the lawyer could rely on name recognition for the request to be considered "forthright."[17]

In 2010, the New York State Bar Committee on Professional Ethics addressed a question similar to that addressed by the Oregon State Bar: is it permissible for a lawyer representing a client during litigation to access

---

11 Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02, 1 (2009), *available at* http://www.philadelphiabar.org/WebObjects/PBAReadOnly.woa/Contents/WebServerResources/CMSResources/Opinion_2009-2.pdf.

12 *Id.*

13 *Id.* at 2. Pennsylvania Rule of Professional Conduct 5.3 states in pertinent part: "With respect to a nonlawyer employed or retained by or associated with a lawyer: . . . (c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if: (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved." PA. RULES OF PROF'L CONDUCT R. 5.3 (2013). Pennsylvania Rule of Professional Conduct 8.4 states in pertinent part: "It is professional misconduct for a lawyer to: . . . (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation" PA. RULES OF PROF'L CONDUCT R. 8.4 (2013). These rules are essentially identical to Rules 5.3 and 8.4 of the ABA Model Rules of Professional Conduct. *See* MODEL RULES OF PROF'L CONDUCT R. 5.3, 8.4 (2013).

14 Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11, at 3.

15 *Id.*

16 *Id.*

17 *Id.*

the public pages of another party's social networking website, such as Facebook or MySpace?[18] The Committee heavily references the 2009 Philadelphia Bar opinion and seems to agree that the relevant rule is that it is professional misconduct for a lawyer to engage in acts involving dishonesty, fraud, deceit, or misrepresentation.[19] The Committee, however, reasons that the rule against deception is not implicated in the specific scenario addressed in its opinion because "the lawyer is not engaging in deception by accessing a public website that is available to anyone in the network, provided that the lawyer does not employ deception in any other way (including, for example, employing deception to become a member of the network)."[20] Consequently, the opinion concludes that a lawyer "may ethically view and access the Facebook and MySpace profiles of a party other than the lawyer's client in litigation as long as the party's profile is available to all members in the network and the lawyer neither 'friends' the other party nor directs someone else to do so."[21] Although this statement seems to prohibit a lawyer from seeking to "friend" other parties, the opinion explicitly qualifies its conclusion by explaining that it does not address the ethical implications of a lawyer seeking to "friend" a represented party or an unrepresented party. The Committee notes, however, that if a lawyer attempts to "friend" a represented party, such conduct would be governed by the rule prohibiting communication with a represented party without prior consent from that party's lawyer, and that if a lawyer attempts to "friend" an unrepresented party, such conduct would be governed by the rule prohibiting lawyers from implying that they are disinterested and requiring them to correct any misunderstandings about their role.[22]

---

18 N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 843 (2010), *available at* http://www.nysba.org/CustomTemplates/Content.aspx?id=5162.

19 *Id.* New York Rule of Professional Conduct 8.4 states in pertinent part: "A lawyer or law firms shall not: . . . (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation." N. Y. RULES OF PROF'L CONDUCT R. 8.4 (2013). This rule is essentially the same as Rule 8.4 of the ABA Model Rules of Professional Conduct. *See* MODEL RULES OF PROF'L CONDUCT R. 8.4 (2013).

20 N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *supra* note 18.

21 *Id.*

22 *Id.* at n.1. New York Rule of Professional Conduct 4.2 states in pertinent part: "In representing a client, a lawyer shall not communicate or cause another to communicate about the subject of the representation with a party the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the prior consent of the other lawyer or is authorized to do so by law." N.Y. RULES OF PROF'L CONDUCT R. 4.2 (2013). This rule is substantially the same as Rule 4.2 of the ABA Model Rules of Professional Conduct, except that the Model Rule does not prohibit the lawyer from "causing another to communicate." *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2013). New York Rule of Professional Conduct 4.3 states in pertinent part: "In communicating on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding."

The New York City Bar Committee on Professional Ethics also issued an opinion in 2010 on the subject of lawyers seeking access to social media content.[23] This opinion addresses "the narrow question of whether a lawyer, acting either alone or through an agent such as a private investigator, may resort to trickery via the internet to gain access to an otherwise secure social networking page and the potentially helpful information it holds," and particularly focuses on the lawyer's "direct or indirect use of affirmatively 'deceptive' behavior to 'friend' potential witnesses."[24] Consistent with New York's "oft-cited policy in favor of informal discovery," the opinion concludes that "an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request" and that the ethical boundaries to "friending" are "not crossed when an attorney or investigator uses only truthful information to obtain access to a website, subject to compliance with all other ethical requirements."[25] A footnote to this conclusion states that the communications of a lawyer and her agents with parties known to be represented by counsel "are governed by Rule 4.2, which prohibits such communications unless the prior consent of the party's lawyer is obtained or the conduct is authorized by law," but does not explicitly conclude that "friending" a represented party constitutes a communication that would violate the rule.[26]

If the attorney or her agent seeks to "friend" an individual under false pretenses (e.g., by creating a fake profile or using false information in the request), the New York City opinion concludes that such activities would violate both the rule prohibiting lawyers from engaging in conduct involving dishonesty, fraud, deceit, or misrepresentation and the rule prohibiting lawyers from knowingly making false statements during the course of representation.[27] Although the Committee acknowledges that other ethics opinions have provided "that deception may be permissible in rare instances when it appears that no other option is available to ob-

---

N. Y. RULES OF PROF'L CONDUCT R. 4.3 (2013). This rule is nearly identical to Rule 4.3 of the ABA Model Rules of Professional Conduct. *See* MODEL RULES OF PROF'L CONDUCT R. 4.3 (2013).

[23] N.Y.C. Bar Ass'n, Formal Op. 2010–2 (2010), *available at* http://www.nycbar.org/ethics/ethics-opinions-local/2010-opinions/786-obtaining-evidence-from-social-networking-websites.

[24] *Id.*

[25] *Id.*

[26] *Id.* at n.4.

[27] *Id.* New York Rule of Professional Conduct 4.1 provides: "In the course of representing a client, a lawyer shall not knowingly make a false statement of fact or law to a third person." N. Y. RULES OF PROF'L CONDUCT R. 4.1 (2013). This rule is essentially the same as Rule 4.1(a) of the ABA Model Rules of Professional Conduct. *See* MODEL RULES OF PROF'L CONDUCT R. 4.1(a) (2013).

tain key evidence," the Committee decides that these limited exceptions are "inapplicable" to social networking websites "because non-deceptive means of communication ordinarily are available to obtain this information" (i.e., the use of formal discovery mechanisms).[28]

In 2011, the San Diego County Bar Legal Ethics Committee issued an opinion explicitly condemning as unethical the act of a sending a "friend" request to parties or witnesses–– represented or unrepresented—where the "friend" request contains the lawyer's real name and no other information.[29] The opinion first focuses on the rule prohibiting a lawyer from communicating with a represented party about the subject of the representation.[30] When a lawyer clicks on the "Add as Friend" button on Facebook, the website sends an automated message to the would-be friend stating, "[lawyer's name] wants to be friends with you on Facebook," and gives the option to accept or decline the request.[31] Although this message is generated by the website and not the attorney, the Committee concludes that it is still "at least an indirect ex parte communication with a represented party" for the purposes of the ethical analysis.[32] As to whether this communication is "about the subject of the representation," the Committee reasons that if the communication "is motivated by the quest for information about the subject of the representation, [then] the communication with the represented party is about the subject matter of that representation" and is therefore prohibited.[33]

The opinion next considers the rule prohibiting a lawyer from engaging in deception and concludes that this duty forecloses a lawyer from seeking to "friend" a witness or party, even if they are unrepresented, without disclosing the purpose of the "friend request."[34] The

---

28 N.Y.C. Bar Ass'n, *supra* note 23.

29 San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

30 *Id.* California Rule of Professional Conduct 2–100 states, in relevant part: "While representing a client, a member shall not communicate directly or indirectly about the subject of the representation with a party the member knows to be represented by another lawyer in the matter, unless the member has the consent of the other lawyer." *Id.* (citing CAL. RULES OF PROF'L CONDUCT R. 2–100 (2011)). Under this rule, communications with a public officer, board, committee, or body; communications initiated by a party seeking advice or representation from an independent lawyer of the party's choice; and communications otherwise authorized by law are permitted. *Id.* This rule is generally the same as Rule 4.2 of the ABA Model Rules of Professional Conduct, except that the Model Rule does not prohibit indirect communications, and the Model Rule does not create exceptions for communications with public entities or communications initiated by a party. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2010).

31 San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1, at 1.

32 *Id.*

33 *Id.* at 1–2.

34 *Id.* Rule 4.1(a) of the ABA Model Rules of Professional Conduct mandates that in the in course of representing a client, a lawyer "shall not knowingly make a false statement of material fact or law to a third person." MODEL RULES OF PROF'L CONDUCT R. 4.1(a) (2013). Model Rule 8.4(c) further prohibits "conduct involving dishonesty, fraud, deceit or misrepre-

opinion relies heavily on the 2009 analysis of the Philadelphia Bar Association Professional Guidance Committee, "notwithstanding the value in informal discovery on which the City of New York Bar Association focused."[35] Interestingly, the opinion notes that "[n]othing would preclude the attorney's client himself from making a friend request to an opposing party or a potential witness in the case" on the ground that the target would recognize the sender by name.[36] This point underscores the opinion's conclusion that a "friend request" by the lawyer is deceptive because such a request seeks "to exploit a party's unfamiliarity with the attorney's identity and therefore his adversarial relationship with the recipient."[37]

Two additional opinions shed light on this topic by examining the use of social media by lawyers searching for information on potential and sitting jurors.[38] The first, issued by the New York County Lawyers' Association (NYCLA) Committee on Professional Ethics in 2011, concludes that it is proper and ethical for a lawyer to undertake a pretrial search of a prospective juror's social networking site and to visit the publicly available sites of a sitting juror as long as the lawyer does not "friend" the juror, subscribe to the juror's Twitter accounts, or "otherwise communicate in any way with the juror or act in any way by which the juror becomes aware of the monitoring."[39] The NYCLA Committee explained that such social media activities are impermissible communications because if a juror becomes aware of a lawyer's efforts to view her social media sites, "it might tend to influence the juror's conduct with respect to the trial."[40] The second opinion, issued by the New York

---

sentation." MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2013). As the opinion acknowledges, California has not incorporated these provisions of the Model Rules into its Rules of Professional Conduct or its State Bar Act. San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1, at 5. The opinion argues, however, that (1) the duty not to deceive judges (contained in California code) arguably stands for a broader duty not to deceive anyone; (2) there is substantial California case law supporting the proposition that lawyers have a duty not to deceive, even outside of the courtroom; and (3) there is a common law duty not to deceive. *Id.* On this basis, the opinion proceeds from the assumption that lawyers are prohibited from engaging in deception. *Id.*

35 San Diego Cnty. Bar Legal Ethics Comm. 2011–2, *supra* note 1, at 6.

36 *Id.*

37 *Id.*

38 *See, e.g.*, N.Y. Cnty. Law. Ass'n Comm. on Prof'l Ethics, Formal Op. 743 (2011), *available at* http://www.nycla.org/siteFiles/Publications/Publications1450_0.pdf; N.Y.C. Bar Ass'n, Formal Op. 2012-2 (2012), *available at* http://www.nycbar.org/ethics/ethics-opinions-local/2012opinions/1479-formal-opinion-2012-02. These opinions are focused on the application of rules that forbid communications between lawyers and jurors, which generally embody stricter "no contact" principles because they prohibit *all* communications, not just those "about the subject matter of the representation." *See* MODEL RULES OF PROF'L CONDUCT R. 3.5 (b) (2013). These opinions, however, still provide insight into how bar committees understand the application of professional conduct rules in the social media context.

39 N.Y. Cnty. Law. Ass'n Comm. on Prof'l Ethics, *supra* note 38, at 1.

40 *Id.*

City Bar Committee on Professional Ethics in 2012, similarly concluded that lawyers may use social media websites for juror research "as long as no communication occurs between the lawyer and the juror as a result."[41] This opinion maintains that if a juror receives a "friend" request (or any other type of invitation or notification) or "otherwise learn[s] of the attorney's viewing or attempted viewing of the juror's pages, posts or comments," this constitutes a "prohibited communication."[42] The Committee defines "communication" as the transmission of information from one person to another, and explains that in the social media context, "friend" requests and other such activities at minimum impart to the targeted juror knowledge that he or she is being investigated. The intent of the attorney using social media is irrelevant.[43]

Most recently, in 2014, the Commercial and Federal Litigation Section of the New York State Bar Association issued a more detailed set of social media guidelines, covering a range of scenarios beyond the discovery realm, although these guidelines are not binding on disciplinary proceedings and do not represent the views of the State Bar Association until they are formally adopted as such.[44] The guidelines continue to distinguish between "public" versus "non-public" portions of a social media profile, and state that a "lawyer may view the public portion of a person's social media profile or public posts even if such person is represented by another lawyer"—including for impeachment purposes.[45] Moreover, the guidelines urge awareness and caution of "unintentional communications," such as LinkedIn notifications that can automatically generate a notice to the person whose profile was viewed.[46] The guidelines recite the normal rule about contact with a represented person, but note in the comments that caution should be used before indirectly accessing social media content, even if the lawyer "rightfully has a right to view it, such as [through] a professional group where both the lawyer and represented person are members or as a result of being a 'friend' of a 'friend' of such represented person."[47] Finally, the guidelines about viewing a represented person's social media profile expressly apply to agents, including "a lawyer's investigator, legal assistant, secretary, or agent and could apply to the lawyer's client as well."[48]

---

41 N.Y.C. Bar Ass'n, *supra* note 23.

42 *Id.*

43 *Id.*

44 COMMERCIAL & FED. LITIG. SECTION, N.Y. STATE BAR ASS'N, SOCIAL MEDIA ETHICS GUIDELINES (2014), *available at* https://www.nysba.org/Sections/Commercial_Federal_Litigation/Com_Fed_PDFs/Social_Media_Ethics_Guidelines.html.

45 *Id.* at 8.

46 *Id.*

47 *Id.* at 9–10.

48 *Id.* at 10.

In considering this group of opinions as a whole, it must first be noted that the opinions are few in number, they come from only a handful of bar associations, and the majority of the bar associations represented are local, not state, associations. The vast majority of state bar associations, including the American Bar Association, have yet to officially weigh in on the subject of informal discovery of social media. Further, there are many points of disagreement amongst this set of opinions. For example, while the New York City Bar considers contact with unrepresented persons by a lawyer or their agent permissible as long as only truthful information is used, the Philadelphia Bar maintains that only direct contact by the lawyer is permissible, while the San Diego County Bar prohibits any such contact.[49] Consequently, one cannot yet rely on these opinions as either comprehensive or authoritative on the question of the ethical permissibility of social media informal discovery.

Several common themes, however, emerge from this set of opinions that may provide insight into how local and state bar associations generally view this issue. First, the opinions generally seem to consider all forms of social media activity to be "communication," although only one opinion explicitly addresses why such activities should be considered "communication" by providing an analytical basis for this conclusion.[50] The remaining opinions appear simply to assume this point. Second, all of the opinions explicitly or implicitly accepted that there is a clear line between "public" and "private" information on social media websites. For example, the Oregon and New York State Bar opinions rely on this distinction by declaring that viewing "public" websites and pages is permissible.[51] The New York City Bar opinion on juror research also relies on this distinction, explaining that "[i]n general, attorneys should only view information that potential jurors intend to be—and make—public."[52] Third, at least three opinions conclude that failure to disclose certain information, such as affiliation with the lawyer or the lawyer's interest in the litigation, constitutes deception, even if only truthful information is provided by the seeker through the use of social media.[53] Only

---

[49] *Compare* N.Y.C. Bar Ass'n, *supra* note 23, *with* Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11, *and* San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

[50] *See* N.Y.C. Bar Ass'n, *supra* note 23.

[51] *See* Or. Bar Ass'n, *supra* note 4; N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *supra* note 18.

[52] *See* N.Y.C. Bar Ass'n, *supra* note 23.

[53] *See* Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11; San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1; N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *supra* note 18.

one opinion comes to a different conclusion,[54] while the remaining opinions are silent on this topic.

B. Practitioners

Given the relative paucity of authority on the ethical boundaries of informal discovery of social media information, practitioners and academics have generally concluded that lawyers should take the most conservative approach to such informal discovery—to limit their research to information that is "publicly available" and not require permission from or notification to the target of the research. For example, one of only a few legal treatises focused on social media definitively states:

> An attorney may not use social media to contact or "friend" a juror or a represented adverse party. These prohibitions also apply to those acting on behalf of the attorney. However, attorneys, like the general public, may view the public portions of anyone's social media site. The one major exception to this rule on viewing public portions of a social media site arises when such viewing constitutes contact. This can happen with social media sites that generate automated responses to the account holder.[55]

Although the treatise acknowledges that the situation is "a little less clear when the attorney or her agent wants to contact via social media an unrepresented party that is likely to be called as a witness," it goes on to explain that jurisdictions take different approaches, and some require full disclosure of the reason for the contact.[56] Similarly, a recent article on the role of social media in litigation, authored by two practicing attorneys, cautions:

> Social media sites are ethical minefields that many lawyers are only now beginning to grapple with. We are probably on safe ground when we access information that users have knowingly made available to the public. Unsurprisingly, courts have accepted that there is no reasonable expectation of privacy in that kind of information. However, it is ethically problematic for lawyers to

---

[54] *See* N.Y.C. Bar Ass'n, *supra* note 23 (concluding that attorneys or their agent may use their real name and profile to send a "friend" request to obtain information from an unrepresented person's social networking website without also disclosing the reason for the request).

[55] PRACTICING LAW INSTIT., *supra* note 2, § 9:6.2.

[56] *Id.*

> "friend" people just to get access to information in their social media profiles.[57]

Countless other publications have issued similar warnings to lawyers seeking to engage in informal discovery of social media.[58] Limiting informal discovery to only publicly available social media information is a quite conservative approach, considering that none of the existing bar opinions mandate such restrictions. Even the most restrictive opinion—the San Diego County Bar opinion—permits lawyers to "friend" unrepresented persons as long as they disclose their interest in seeking the information.[59] This risk-averse approach is both understandable and wise, however, considering the serious consequences, both professional and personal, that can result from committing an ethical violation. Until the ABA and the state bars issue clear rules and guidance explicitly delineating ethical boundaries for informal discovery of social media, practitioners will likely continue to refrain from all but the most circumspect uses of this valuable source of information.

C. Courts

To our knowledge, courts have not directly ruled on the extent to which the rules of professional conduct limit informal discovery of social media information. Some courts have addressed related topics, including the admissibility of evidence gathered through informal discovery of social media sites, the scope of formal discovery of social media information, and the implications of other laws (such as the Stored Communications Act, 18 U.S.C. § 2701 (2002)) on the collection of social media information.[60] These cases, however, do not apply the rules

---

[57] Radhakant & Diskin, *supra* note 2.

[58] *See, e.g.*, Justin P. Murphy & Matthew A. Esworthy, *The ESI Tsunami: A Comprehensive Discussion about Electronically Stored Information in Government Investigations and Criminal Cases*, CRIM. JUST., Spring 2012, at 31, 34 (noting that lawyers "can run afoul of ethics rules when they use social media to gather evidence that is not publicly available"); *Social Networking Sites Are Valuable Tools for Lawyers: But Beware the Potential Ethical Pitfalls*, INTERNET FOR LAWYERS, http://www.netforlawyers.com/content/social-networking-sites-are-valuable-tools-lawyers-beware-potential-ethical-pitfalls (last visited Aug. 22, 2014) (discussing the Philadelphia Bar opinion, and oting that such ethical dilemmas can be avoided by limiting such research to public profiles only, since "there would be no actual contact or exchange with the profile's owner").

[59] San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

[60] *See, e.g.*, Griffin v. Maryland, 19 A.3d 415, 423–24 (Md. 2011) (holding that trial court abused its discretion by admitting into evidence pages printed from MySpace that were not appropriately authenticated); Tienda v. State, 358 S.W.3d 633, 642, 647 (Tex. Crim. App. 2012) (concluding that because there was sufficient circumstantial evidence to authenticate photographs taken from defendant's MySpace profile, the evidence was properly admitted); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 977–990 (C.D. Cal. 2010) (analyzing whether social-networking sites "fall within the ambit" of the Stored Communications Act); Romano v. Steelcase, 907 N.Y.S.2d 650 (App. Div. 2010) (considering scope of permissible discovery of social media information).

of professional conduct in a disciplinary context, and it is well established that ethical and evidentiary rulings do not necessarily run parallel to each other. Consequently, although such cases might inform our understanding of the courts' views on the subject, they do not provide a clear answer as to what conduct is ethically permissible.

II. A BETTER VIEW: INFORMAL DISCOVERY OF SOCIAL MEDIA INFORMATION IS BROADLY PERMISSIBLE UNDER THE CURRENT RULES OF PROFESSIONAL CONDUCT

The prevailing view that ethical obligations constrain informal discovery of social media information to that which is publicly available relies on several misconceptions that reflect a poor understanding of both the nature of social media and the underlying purposes of the relevant rules of professional conduct. First, this view rests on a false premise that a clear distinction can be made between what is "public" and what is "private" on any given social media website. In fact, the blurry line between public and private information that exists in most, if not all, social media contexts makes it impossible to rely effectively on this distinction as the basis for a rule lawyers can easily follow. Further, it is unclear how the concept of "privacy" is germane to ethical inquiries under the relevant rules of professional conduct.

Second, the existing bar opinions miscategorize social media activities as "communications" within the meaning of the relevant rules of professional conduct based on partial and ill-fitting analogies to communications in the physical (i.e., non-virtual) world. Social media enable users to share information in novel and unique ways, and consequently, social media activities are not easily transplanted into "real-world" scenarios. To properly analogize social media activities to real-world interactions, the specific function of each type of activity must be understood in the context of the application within which it operates—the existing bar opinions fail to do this.

Third, the existing bar opinions limit their analyses of the relevant rules of professional conduct to determining whether certain social media activities fall under the definitional meaning of specific words within the rules, such as "communication" or "deception." Instead, the bar opinions could analyze whether the social media activity at issue offends the underlying purposes of each relevant rule and tie their conclusions and rulings to these purposes accordingly.

As a result of these misconceptions and analytical missteps, the prevailing view is unnecessarily restrictive. In fact, the existing rules of professional conduct allow for broad and extensive informal discovery of social media information. Properly analyzed and applied, these rules prohibit only the use of explicit fraud and misrepresentation by lawyers

seeking social media information (e.g., creating fake identities or profiles) and direct questioning of targets via social media.

A. Public vs. Private: How Clear Is the Line and Is it Important?

As detailed above, the prevailing view pressed by practitioners and bar associations alike relies on a clear distinction between "public" and "private" social media information.[61] Most of the bar opinions and practitioner publications do not explain precisely what the term "public" encompasses, but instead simply presume the term speaks for itself.[62] The few sources that address the meaning of "public" conclude that where attorney conduct moves beyond viewing social media information into contact with the research target, then it is likely the information is "non-public" (or, in other words, "private").[63] This definition does very little in the way of drawing a clear line between public and private social media information—largely because it is impossible to draw such a line due to the intrinsic nature of social media. The sheer number and diversity of social media applications and websites, constant innovations in social media, layers of information sharing possible via social media, transferability of information between social media users, and many other factors contribute to the inherent blurriness between "public" and "private" social media information. The existing bar opinions and treatises assume not only that the public-private divide makes sense, but also that the line between them can be drawn clearly and easily in any social media context.[64] In reality, this line cannot be drawn clearly or easily and should not govern the extent to which informal discovery of social media is ethically permissible. Even if it were possible to draw a clear line between the two, the bar opinions and practitioner publications fail to explain why or how the designation of information as "public" or "private" should be a relevant consideration in the application of the cited rules of professional conduct. This further supports our contention that the ethical rules governing informal discovery of social media information should not rest on the fictitious distinction between public and private.

"Social media" is generally defined as "a group of Internet-based applications . . . that allow the creation and exchange of User Generated Content."[65] The term "social media," therefore, does not refer to a single

---

61 *See supra* Part I.A.

62 *See, e.g.*, N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *supra* note 18; Radhakant & Diskin, *supra* note 2, at 17–22.

63 San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1; N.Y. Cnty. Law. Ass'n Comm. on Prof'l Ethics, *supra* note 38; *see, e.g.*, PRACTICING LAW INST., *supra* note 2, at 9:32–33.

64 *See, e.g.*, San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

65 Andreas M. Kaplan & Michael Haenlein, *Users of the World, Unite! The Challenges and Opportunities of* Social Media, 53 BUS. HORIZONS 59, 61 (2010); *Social Media Definition*,

method of information sharing, but rather encompasses potentially infinite different modes. At present, there are hundreds of social media platforms[66] and more than a billion accounts, or profiles, on Facebook and other websites.[67] As a group of scholars explains, "[t]here currently exists a rich and diverse ecology of social media sites, which vary in terms of their scope and functionality."[68] Each of these thousands of social media websites operate independently and uniquely—governed by their own individual policies for membership, information sharing, privacy, and notification.

This diversity presents the first problem with the practical application of the public-private distinction: how lawyers are supposed to determine which information on any given website is "public" if this designation depends on how each site functions. It is not reasonable to expect lawyers, courts, and bar committees tasked with implementing the rules of professional conduct to know and understand the intricate inner workings of these thousands of social media websites. Under the prevailing view, such knowledge is necessary in order to undertake any informal discovery[69]—otherwise, lawyers will not know if even viewing a profile, such as on LinkedIn, will trigger a notification. Such knowledge would also be necessary for lawyers who intend to object to informal discovery undertaken by the opposition, and for a court or bar committee seeking to enforce ethical rules. The bar opinions on which this prevailing view is based focus their analyses on a few well-known sites—namely, Facebook, MySpace and Twitter. These opinions assume that their Facebook-specific determinations can be easily applied to other social media platforms and websites, and expect lawyers to discern the operational equivalent of "friending" for other websites they may want to explore—an approach that is likely to produce inconsistent results. Even

---

OXFORD DICTIONARIES, http://www.oxforddictionaries.com/us/definition/american_english/social-media (last visited Aug. 22, 2014) (defining social media as "websites and applications that enable users to create and share content or to participate in social networking.").

66 *See* Richard Hanna, Andrew Rohm & Victoria L. Crittenden, *We're All Connected: The Power of the Social Media Ecosystem*, 54 BUS. HORIZONS 265, 266 (2011) (explaining that social media platforms include social networking, text messaging, photo-sharing, podcasts, video-streaming, wikis, blogs, discussion boards, micro-blogging, and location-based tools).

67 *See* Jemima Kiss, *Facebook's 10th Birthday: From College Dorm to 1.23 Billion Users*, THE GUARDIAN, Feb. 3, 2014, http://www.theguardian.com/technology/2014/feb/04/facebook-10-years-mark-zuckerberg; Ingrid Lunden, *Twitter May Have 500M+ Users But Only 170M Are Active, 75% On Twitter's Own Clients*, TECHCRUNCH (July 31, 2012), http://techcrunch.com/2012/07/31/twitter-may-have-500m-users-but-only-170m-are-active-75-on-twitters-own-clients/; *Skype Grows FY Revenues 20%,Reaches 663mln Users*, TELECOMPAPER (Mar. 8, 2011), http://www.telecompaper.com/news/skype-grows-fy-revenues-20-reaches-663-mln-users—790254.

68 Jan H. Kietzmann et al., *Social Media? Get Serious! Understanding the Functional Building Blocks of Social Media*, 54 BUS. HORIZONS 241, 242 (2011).

69 *E.g.*, N.Y.C. Bar Ass'n, *supra* note 23 ("It is the duty of the attorney to understand the functionality and privacy settings of any service she wishes to utilize for research.").

the bar opinions and practitioner publications that seek to provide some broader guidance by defining "private" information, as that which requires some kind of contact, acknowledge the uncertainty implicit in this rule due to confusion or lack of awareness regarding the functionality of social media websites.[70]

This concern could be laid to rest perhaps by adding a corollary to the public-private rule requiring lawyers to learn the operational details of any social media website they intend to use.[71] Even assuming, however, that lawyers *should* be responsible for learning the operational details of every social media website that they or their opponent make use of during a case, the fact that such websites are constantly changing their operations and policies presents another obstacle for lawyers trying to figure out what information is "public."[72] Social media websites are by their very nature innovative—their success or failure depends in large part on their ability to adapt to changing interests and trends. To accurately determine what is "public" social media information, lawyers will have to constantly update their knowledge of social media websites. For example, in its nine-year history, Facebook has made countless changes to many core aspects of the site, including multiple changes to its classification system for personal data, search features, data visibility restrictions, and privacy policies.[73] As a result, the line between public and

---

70 N.Y. Cnty. Law. Ass'n Comm. on Prof'l Ethics, *supra* note 38 ("Moreover, under some circumstances a juror may become aware of a lawyer's visit to the juror's website . . . the contact may well consist of an impermissible communication."); N.Y.C. Bar Ass'n, *supra* note 39 ("Even if the attorney does not intend for or know that a communication will occur, the resulting inadvertent communication may still violate the Rule."); PRACTICING LAW INST., *supra* note 2, at 9–33 (acknowledging a lack of certainty in the ethical implications of "situations where the attorney was ignorant or unaware of the automatic response procedures" of a social media website).

71 However, this would not help lawyers with the burden of learning about social media websites used by the opposition. Further, courts and bar committees would still need more comprehensive knowledge in order to have an informed view of what is public and private information.

72 *See, e.g.*, Joe Nocera, *Facebook's New Rules*, N.Y. TIMES, Oct. 18, 2013, http://www.nytimes.com/2013/10/19/opinion/nocera-facebooks-new-rules.html ("In its short nine-year existence, Facebook has made many changes to its privacy policies . . . .").

73 *See id.*; *see also* Mandy Gardner, *Facebook Privacy Settings Are Changing Again*, GUARDIAN LIBERTY VOICE (Oct. 30, 2013), http://guardianlv.com/2013/10/facebook-privacy-settings-are-changing-again/ ("Facebook profiles will no longer be invisible to certain people unless they have already been officially blocked by other users. Site administrators say the reason for the Facebook privacy changes is the fact that there are now so many different ways for a profile to be discovered on the site. For example, one's profile might be seen through a tagged photo, group comments or via the new Graph Search feature. When the 'Who can look up your timeline' feature was introduced, a name-search was the only way to find someone's profile. With the modernization of the site, this feature is all but obsolete."); Matt McKeon, *The Evolution of Privacy on Facebook*, MATTMCKEON.COM (April 2010), http://mattmckeon.com/facebook-privacy/ ("Facebook's classification system for personal data has changed significantly over the years" and "Facebook hasn't always managed its users' data well. In the beginning, it restricted the visibility of a user's personal information to just their friends and

private information on Facebook has shifted repeatedly, with specific types and pieces of information changing from private to public and back to private again. The expectation that lawyers will keep up with constant policy changes for dozens if not hundreds of different websites is unrealistic and unreasonably burdensome.

The "gray areas" of social media websites create yet another problem for lawyers trying to identify the line between public and private social media information. Such "gray areas" include methods of accessing information without requesting permission from the subject of the investigation or that do not result in a notification to the subject, but that do require the investigating lawyer to take some active steps to obtain the information.[74] For example, on Facebook, users can join "groups"—pages created within the site that are based around a particular interest, topic, affiliation, or association. By joining the same groups as the research target, an investigating lawyer may be able to view postings made by the target on the group pages, and learn about the target's interactions and relationships with other members of the groups. To join these groups, the lawyer normally would not need to request permission from the target nor would a notification be sent to the target. The target would, however, be able to see that the lawyer was a member of the group by browsing the group's list of members. An investigating lawyer could also gather information about a target by friending the target's friends and family. In so doing, the lawyer would be able to see any postings made by the target on the walls of these friends and family, and see any photos of, or comments to, the target they posted. Again, the lawyer would not need the permission of the target, and the target would not receive any personal notification, though the target would be able to see from any friend or family member's pages that the lawyer had friended them. Such information is neither wholly public, because the lawyer must take action to gain access to it, nor wholly private as to the target of the research, because the target does not control access to it. The New York State Bar Association guidelines on social media, which most directly address methods such as "friend of a friend" network research, consider these methods to be gray areas: the guidelines essen-

---

their 'network' (college or school). Over the past couple of years, the default privacy settings for a Facebook user's personal information have become more and more permissive. They've also changed how your personal information is classified several times, sometimes in a manner that has been confusing for their users."); Kurt Opsahl, *Facebook's Eroding Privacy Policy: A Timeline*, ELECTRONIC FRONTIER FOUNDATION (Apr. 28, 2010), https://www.eff.org/deeplinks/2010/04/facebook-timeline ("Since its incorporation . . . Facebook has undergone a remarkable transformation. When it started, it was a private space for communication with a group of your choice. Soon, it transformed into a platform where much of your information is public by default. Today, it has become a platform where you have no choice but to make certain information public . . . .").

74 *See* Gardner, *supra* note 73; *see also* McKeon, *supra* note 73.

tially just urge caution and expressly note that—even in the stricter juror context—ethics opinions "have not directly addressed" non-deceptive viewing of putatively private social media information through alumni groups.[75] Overall, the existence of such "gray areas" reveals the fiction of a clear and easy line between public and private social media information and the impracticality of directing lawyers to conform their conduct along it.[76]

Questions surrounding the timing of requests for information also confound the simple labeling of social media information as either public or private. Several bar opinions have determined that it is impermissible to seek social media information via a third party, i.e., a lawyer cannot ask an apparently neutral third party to friend the target on the lawyer's behalf as a way to avoid the alleged "communication" of a direct friend request.[77] Practitioners seem to conclude that by strictly adhering to the public-private rule, they will avoid any potential ethical problems involving third parties. It is unclear, however, what ethical implications arise from requesting information from a third party who is already connected to the research target before the lawyer is aware of or involved in the litigation. For example, the lawyer could ask a third party who is Facebook friends with the target to provide copies of the target's profile and all of their postings, or the lawyer could ask a third party who follows the target on Twitter to provide copies of all of the target's tweets. This information can hardly be considered "public," since access to it is restricted to the target's friends or followers. Neither is this information clearly "private" (as vaguely defined in bar opinions and practitioner publications) since the lawyer has not contacted the target to obtain it and the target has chosen to share it with the third party.[78] This scenario demonstrates the difficulty of definitively labeling social media information as either public or private because the nature of the information may change as it is transferred from user to user. Further, this scenario highlights the confusion inherent in the public-private rule that results in overbroad restrictions on lawyers seeking informal discovery of social

---

[75] COMMERCIAL & FED. LITIG. SECTION, N.Y. STATE BAR ASS'N, *supra* note 44, at 10, 15–16.

[76] In addition, commercial data aggregation services that "crawl" the web and cull information from an array of databases and sources, including social media sites, in order to generate reports about persons and companies are now widely available, further blurring the line between public and private social media information. *See* Lori Andrews, *Facebook Is Using You*, N.Y. TIMES, Feb. 4, 2012, http://www.nytimes.com/2012/02/05/opinion/sunday/facebook-is-using-you.html.

[77] *See, e.g.*, Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11; N.Y. State Bar Ass'n Comm. on Prof'l Ethics, *supra* note 18; *see also* COMMERCIAL & FED. LITIG. SECTION, N.Y. STATE BAR ASS'N, *supra* note 44.

[78] *See, e.g.*, PRACTICING LAW INST., *supra* note 2, § 9:6.2; N.Y. Cnty. Law Ass'n Comm. on Prof'l Ethics, *supra* note 38; San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

media information. In other words, by limiting their research to public information only, lawyers yield access to information that while not strictly "public," does not require the supposedly unethical "communication" with the research target that justifies the prohibition on so-called "private" information, and therefore should be accessible to lawyers.

Finally, this examination of the many complexities and uncertainties intrinsic to the prevailing view begs the question: even if one were willing to parse out the specific distinction between public and private social media information for every possible scenario, why does this public-private divide matter and why should it define the limits of permissible informal discovery of social media information? The bar opinions appear to be motivated in part by concern regarding the personal privacy of social media users.[79] This concern is somewhat misplaced. The rules of professional conduct are not concerned with enshrining a robust conception of third-party privacy. Rather, the overarching purpose of the rules of professional conduct is to provide guidance to lawyers as to the responsible practice of law, to protect the interests of clients in the context of engaging the services of a lawyer, and to provide standards for bar discipline.[80] To these ends, each rule is crafted to either promote specific actions or results, or to prohibit certain actions and avoid particular outcomes. The rules at issue in the context of social media informal discovery—the rules prohibiting communicating with represented parties, misleading unrepresented persons to believe one is disinterested, and committing fraud or deceit—are all focused on preventing specific outcomes. An understanding of these purposes should guide any analysis of these rules, as will be discussed in Part II.C below. These rules are aimed at preventing abuse and trickery, not at protecting the privacy of individuals, and therefore consideration of privacy as a factor is inappropriate when applying these rules to the social media informal discovery context. Further, as numerous courts have recognized in the context of formal discovery, the very purpose of social media websites is to share information with others—rendering such information inherently *not* private and concerns over protecting the privacy of social media users even less relevant.[81]

---

79 *See, e.g.*, San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1 (concluding that the Committee's interpretation of the rules of professional conduct "strikes the right balance between allowing unfettered access to what is public on the Internet about the parties without . . . surreptitiously circumventing the privacy even of those who are unrepresented").

80 *See generally* MODEL RULES OF PROF'L CONDUCT, Preamble & Scope (2012).

81 *See, e.g.*, *Romano*, 907 N.Y.S.2d 650, 657 (App. Div. 2010) (compelling discovery of plaintiff's Facebook and MySpace accounts despite plaintiff's privacy objections, noting that sharing personal information with others is "the very nature and purpose of these social networking sites" and that "in this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking") (internal quotation marks omitted).

B. Real-World Analogies: What Constitutes "Communication About the Subject of the Representation"?

Central to the bar opinions' reasoning is the idea that social media activities are "communications" within the meaning of, and prohibited by, the relevant rules of professional conduct.[82] In explaining this point, the bar opinions offer various analogies intended to demonstrate that social media activities are such communications. Rather than confirm their reasoning, however, these inapposite analogies undermine the bar opinion analyses by often revealing a poor understanding of the nature of social media. For example, the Philadelphia Bar opinion compares the act of a third party using only truthful information to send a Facebook friend request to a research target on behalf of a lawyer without disclosing the relationship to the lawyer to an individual pretending to be a utility worker in order to place a hidden video camera inside the target's home—an act which is clearly deceptive, and therefore prohibited.[83] This analogy is problematic for several reasons. First, the third party is using only truthful information in their friend request.[84] Although the third party is not disclosing their relationship with the lawyer to the research target, the third party is not hiding nor lying about it either.[85] This conduct seems fairly far removed from wearing a disguise and falsely claiming to be a utility worker. Second, this analogy fails to recognize the difference between installing a hidden camera in a person's home in order to capture information that the research target has no idea that they are sharing, and making a friend request, which, if granted, allows the third party access only to information that the target chooses to share with friends. The former activity is spying and requires a passive target who makes no decision to share information with the third party; the latter activity is observation and requires a target who actively chooses to grant access to the third party and others and actively chooses to post comments, photos, videos, etc. Further, a hidden camera in the home cannot distinguish between the different types of information it may capture. For example, a hidden camera in the living room may capture some information the target intends to share with others (e.g., the target's conversation during a party), or it may capture deeply private information (i.e. things the target says or does when the target believes he or she is completely alone). On Facebook, the third party will only have access to

---

82 *See, e.g.*, Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11 (describing the act of a third party sending a Facebook friend request to a potential witness as a "communication"); San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1 (concluding that a Facebook friend request constitutes "an open-ended inquiry to a represented party in cyberspace seeking information about the matter outside the presence of opposing counsel").

83 Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11.

84 *See id.*

85 *Id.*

information that the target intends to share; it is not possible for the third party to access truly private information without the target's knowledge or consent, simply because they are "friends."[86] Third, this analogy overlooks a critical distinction between the types of spaces involved. The law recognizes the home as a sacred space, where one has the right to be free from unwanted intrusions from outsiders.[87] There are few, if any, spaces where privacy is more protected than the home.[88] Obviously, sharing information with and exposing one's private activities to others is not the primary purpose of having a home. In stark contrast, the internet generally, and social networking sites specifically, are not considered sacred or particularly private spaces in any sense. Indeed, the principal reason social networking sites exist is to connect and share information with large numbers of other people. To compare this virtual public forum with a place as private as the home is far-fetched.

The San Diego bar opinion includes several similarly troubling analogies. In attempting to support its conclusion that any social media activity involving a represented party constitutes an impermissible communication about the subject matter of the representation, the Committee draws analogies to two recent federal cases.[89] In *United States v. Sierra Pacific Industries*, an action brought by the government alleging corporate responsibility for a forest fire, counsel representing a corporation attended a Forest Service event open to the public and questioned Forest Service employees about fuel breaks, fire severity, and other related topics.[90] The court rejected the counsel's defense that he was exercising his right to petition the government for redress of grievances, finding instead that he was "attempting to obtain information for use in the litigation," and concluded that his conduct violated the rule prohibiting communication with represented parties about the subject matter of the representation.[91] The Ethics Committee points to this conclusion as evidence that the lawyer's purpose in sending the friend request is critical to the ethical inquiry and because the lawyer "hopes" the friend request will lead to information relevant to the litigation, such communication is "about the subject of the representation" and therefore prohibited.[92] The Committee likens the friend request to any other "open-ended [or] generic question[ ]" asked during the course of litigation to "impel the other side to

---

86 *Statement of Rights and Responsibilities*, FACEBOOK (April 12, 2014) https://www.facebook.com/legal/terms.

87 *See, e.g.*, Georgia v. Randolf, 547 U.S. 103, 123–24 (2006) (Stevens, J., concurring) (finding a right "[a]t least since 1604" to exclude governmental officials and others from the home when they do not have a valid warrant).

88 *See id.*

89 San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

90 United States v. Sierra Pacific Indus., 759 F. Supp. 2d 1206, 1208 (E.D. Cal. 2010).

91 *Id.* at 1213–14.

92 San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

disclose information that is richly relevant to the matter."[93] Both this comparison and the analogy to *Sierra Pacific* are inapposite to the friend request scenario. There is an obvious distinction between directing specific questions to the target, and requesting access to postings made at the target's own initiative. In *Sierra Pacific*, the Forest Service employee provided information that he would not have provided otherwise due to the direct questions of the lawyer.[94] In the Facebook scenario, the lawyer is asking only for access to information that has already been posted by the target, and that will be posted regardless of whether the lawyer has access.[95] This scenario is more comparable to the lawyer signing up to attend the Forest Service event, but not speaking or asking questions—activities that neither the *Sierra Pacific* court nor the Committee suggest are impermissible. If the lawyer posted questions or comments on the target's Facebook page, then *Sierra Pacific* might be a suitable analogy. The comparison to other "open-ended" questions is similarly problematic in that it involves asking a question that will elicit information from the target that would not otherwise be provided. Context is also important—asking any question "during litigation" (e.g., during a meeting, deposition, or negotiation) is implicitly about the litigation and is generally likely to elicit information particularly relevant to the litigation. Social media websites, however, are general forums, where individuals provide information on whatever topic they desire and the nature of the information provided is either unaffected by the lawyer's access, or is *less* likely to be about the subject of the litigation because of the lawyer's access.

In the second case referenced by the San Diego Committee, *Midwest Motor Sports v. Arctic Cat Sales, Inc.*, a lawyer sent a private investigator into the opposing party's showroom to question and surreptitiously record their employees talk about their sales volumes and sales practices.[96] The court determined that the lawyer violated the ethical rule prohibiting ex parte communication with represented parties, even though the investigator did not question the employees directly about the litigation, because the questioning related to sales information which may have been relevant to the issue of damages.[97] The Committee considers the lawyer's conduct in this case to be essentially the same as a lawyer attempting to collect information relevant to the litigation by friending the opposing party and condemns both as ethically impermissible.[98] To bolster the point that the lawyer or her agent need not ask

---

93 *Id.*
94 *Sierra Pacific Indus.*, 759 F. Supp. 2d at 1208.
95 San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.
96 Midwest Motor Sports v. Arctic Cat Sales, Inc., 347 F.3d 693, 695 (8th Cir. 2003).
97 *See id.* at 699.
98 *See* San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

directly about the litigation for the communication to be "about the subject of the representation," the Committee argues that a defense lawyer asking a plaintiff generally about recent activities during a deposition, in order to obtain evidence relevant to whether that plaintiff failed to mitigate damages, is clearly asking about "the subject of the representation."[99] Concluding that such questioning is "qualitatively no different from an open-ended inquiry to a represented party in cyberspace seeking information about the matter," the Committee determines that the former conduct is appropriate, whereas the lawyer's conduct in *Midwest Motor Sports* and in the Facebook scenario is not because it is outside the presence of opposing counsel and discovery procedures do not sanction it.[100] These comparisons fail for the same reasons that the *Sierra Pacific* analogy fails: (1) both *Midwest Motor Sports* and the hypothetical deposition involve lawyers asking direct questions to obtain information that would not otherwise have been provided—the Facebook scenario does not involve asking this type of question; and (2) even general deposition questions (interactions that would not occur but for the litigation) are implicitly about the subject of the litigation, there is no such implicit connection in a Facebook friend request.[101] Further, the employees in *Midwest Motor Sports* did not consent to being recorded and could not reasonably have expected such conduct by the lawyer.[102] In contrast, a target granting the friend request of a lawyer (or stranger) gives consent and has full knowledge that the lawyer will be able to view and record all of the information on their Facebook page.[103]

These analogies also reveal a worrisome lack of familiarity with social media. Some bar committees erroneously assume that requests for access via social media websites can be simply translated into their "real world" equivalents by imagining the requests as verbal communications between individuals (i.e., the lawyer and the research target).[104] In attempting to force social media interactions into preexisting categories of communication, bar committees fail to consider that social media can provide entirely novel and unique modes of sharing information that do not lend themselves easily to "real world" translations.[105] To begin with, social media users generate information with the primary purpose of sharing this information in a non-specific way with groups, not individu-

---

99 *Id.*

100 *Id.*

101 *See id.*

102 *See Midwest Motor Sports*, 347 F.3d at 695.

103 *See* San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

104 *See id.*

105 *See id.*

als.[106] This is unlike any scenario involving "real world" oral or written communications, which generally require the speaker or writer to consciously direct his words to an individual or a selected group of individuals.[107] Although social media users may restrict access to their websites to a certain group of individuals, this is not usually a choice users make with every post, comment, or tweet.[108] Instead, social media users essentially permit others to join their "group" (e.g., as a Facebook friend or a follower on Twitter), and then, in a completely separate act, choose to broadcast information to that group as a whole.[109]

Therefore, the lawyer is not engaging in an interactive, individualized, or dialogue-based communication with the target in seeking access to this information. Rather, the lawyer is requesting permission to join the membership-based public forum in which the target chooses to share information with a group of individuals. Consequently, this type of social media activity is not as much a verbal communication as it is more analogous to conduct such as signing up for a subscription-based newsletter or buying tickets for a speaking event. In these latter scenarios, the lawyer requests access to a limited forum in which the information at issue is promulgated regardless of the lawyer's action. If these activities are ethically permissible—and there is no reason to think they are not[110]—then the analogous social media activity should be similarly permissible.

Finally, to the extent such social media activities can be considered verbal in nature, they are akin to introductions and not general requests for information. Notification messages and access requests simply inform the research target that the lawyer is, or would like to be in, the target's social media space and be able to observe their conduct (e.g., posts, tweets, etc.).[111] In substance, this is no different from a lawyer introducing him or herself to a target and saying nothing further (which is clearly permissible) and is far from a general request for information.[112] This critical distinction arises, again, from the fact that targets produce and publish social media information on their own initiative regardless of the lawyer's access. In the real-world scenarios envisioned by bar committees, no matter how general the question, the target's reply

---

106 *See, e.g.*, *How Sharing Works*, FACEBOOK, https://www.facebook.com/about/sharing (last visited Sept. 20, 2014); *Learn the Basics*, TWITTER, https://discover.twitter.com/learn-more (last visited Sept. 20, 2014); *Who Can See Your Posts*, GOOGLE+, https://support.google.com/plus/answer/1053543?hl=en (last visited Sept. 20, 2014).

107 *See* San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

108 *See, e.g.*, *How Sharing Works*, *supra* note 106; *Who can See Your Posts*, *supra* note 106.

109 *Id.*

110 *See* San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

111 *Id.*

112 *Id.*

(i.e., the production of the information) is prompted by the lawyer's question.[113] By prohibiting these social media introductions, bar committees expand the ban on ex parte communications to cover all communications, not just those about the subject of the representation, which is clearly outside the scope of the rule.[114] Further, applying such an overbroad restriction to informal discovery of social media information is unreasonable and impractical considering the growing presence and importance of social media in everyday life.[115]

C. Applying the Rules: What Are the Underlying Purposes of the Relevant Rules of Professional Conduct?

The various bar opinions that conclude that informal discovery of non-public social media information violates the rules of professional conduct[116] are generally based on the bar committees' application of three particular rules: (1) the rule prohibiting communication with a represented party about the subject matter of the representation outside the presence of that party's counsel; (2) the rule prohibiting lawyers from stating or implying that they are disinterested in the subject matter to an unrepresented person; and (3) the rule prohibiting a lawyer from engaging in conduct involving dishonesty, fraud, deceit, or misrepresentation.[117] As discussed extensively in the preceding sections, these bar opinions erroneously limit their analyses of these rules to the definitional meaning of specific words within them, such as "communication" or "deception," by way of inapposite "real world" analogies.[118] As a result, the prevailing view that the rules of professional conduct limit informal discovery of social media information to that which is publicly available is unnecessarily and impracticably restrictive. A close examination of the underlying purposes of each of the three rules and careful consideration of whether the social media activities at issue offend these purposes reveal that, in fact, the existing rules of professional conduct allow for broad and extensive informal discovery of social media information, and prohibit only the use of explicit fraud and misrepresentation in seeking social media information (e.g., creating fake identities or profiles) and direct questioning of targets via social media.

---

113 *See, e.g.*, Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11, at 3; San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

114 *See* San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

115 *See, e.g.*, *10 Years of Social Media Mania & The 2014 Statistics*, DUBAI CHRONICLE (March 20, 2014), http://www.dubaichronicle.com/2014/03/20/10-year-social-media-mania-2014-statistics/.

116 *See, e.g.*, Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11, at 3; San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

117 *See supra* Part II.A.

118 *See supra* Part II.A–B.

1. ABA Model Rule of Professional Conduct 4.2

Rule 4.2 of the ABA Model Rules of Professional Conduct[119] states as follows:

> In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.[120]

Rule 4.2 serves three primary functions: (1) to protect represented persons from "overreaching by other lawyers who are participating in the matter;"[121] (2) to prevent other lawyers from interfering with and adversely affecting the lawyer-client relationship between represented persons and their chosen counsel;[122] and (3) to reduce the likelihood that represented persons "will disclose privileged or other information that might harm their interests."[123] Rule 4.2 "presumes generally" that represented persons are "not legally sophisticated and should not be put by an opposing lawyer in the position of making uninformed decisions or statements or inadvertent disclosures" that are harmful to their interests.[124] In short, the purpose of Rule 4.2 is "to prevent a skilled advocate from taking advantage of a non-lawyer."[125]

In examining Rule 4.2, courts generally have espoused these rationales.[126] For example, one New York federal court describes the policies behind the rule as preventing "unprincipled attorneys" from "exploiting the disparity in legal skills between attorney and lay people;" "circum-

---

119 For purposes of this argument, this Article will analyze the rules of professional conduct as articulated in the ABA Model Rules of Professional Conduct. Although the bar opinions discussed in Part II and referred to in Part III apply the rules of professional conduct of their respective states, these rules are generally modeled on and are often identical to the ABA Model Rules. As of this writing, all fifty states, with the exception of California, the District of Columbia, and the U.S. Virgin Islands have adopted the ABA Model Rules of Professional Conduct in some form. *Model Rules of Professional Conduct*, AM. BAR ASS'N, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct.html (last visted Aug. 22, 2014).

120 MODEL RULES OF PROF'L CONDUCT R. 4.2 (2013).

121 *Id.* at cmt. 1.

122 *Id.*; *see also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-396 (1995).

123 ABA Comm. on Ethics & Prof'l Responsibility, *supra* note 122; *see also*, MODEL RULES OF PROF'L CONDUCT R. 4.2 cmt. 1 (2013).

124 ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-443 (2006).

125 *Id.*

126 *See* CTR. FOR PROF'L RESPONSIBILITY, AM. BAR ASS'N, ANNOTATED MODEL RULES OF PROF'L CONDUCT § 4.2 , at 406–407 (Bennett et al. eds., 7th ed. 2011); *see, e.g.*, Polycast Tech. Corp. v. Uniroyal, Inc., 129 F.R.D. 621, 625 (S.D.N.Y. 1990), Jenkins v. Wal-Mart Stores, Inc., 956 F. Supp. 695, 696 (W.D. La. 1997).

venting opposing counsel to obtain unwise statements from the adversary party;" and "driving a wedge between the opposing attorney and that attorney's client," in addition to protecting against the "inadvertent disclosure of privileged information."[127] Similarly, a Louisiana federal court explains that the "dual purposes behind Rule 4.2 are to prevent disclosure of attorney/client communications, and to protect the party from 'liability-creating' statements elicited by a skilled opposing attorney."[128]

Banning all communications between lawyers and represented persons is explicitly *not* the objective of Rule 4.2. The scope of Rule 4.2 is limited to communications related to the subject matter of the representation, and the rule therefore contemplates a matter that is "defined and specific, such that the communicating lawyer can be placed on notice of the subject of the representation."[129] Consequently, communications concerning matters outside this "defined and specific" representation are perfectly permissible.[130]

Considering these purposes, it is apparent that, under the prevailing view, the social media activities at issue do not run afoul of Rule 4.2. To be clear, the social media activities referred to include requesting permission to access the research target's social media website using the lawyer's real identity and profile (e.g., a Facebook friend request) and automated notifications to the research target that the social media website is being viewed (e.g., a Twitter notification), but do not include any further communications (e.g., posting questions or comments to the target). First, Rule 4.2 is largely focused on preventing lawyers from "eliciting" information from represented persons.[131] In the social media context, no information is being "elicited." Rather, the lawyer is merely asking to view information that the represented person chooses to post at her own initiative for her audience to view, regardless of the lawyer's ability to access this information. Such passive observation is not the type of conduct the rule is aimed at preventing; only active engagement with the represented person triggers the operation of Rule 4.2.[132]

Second, the request for access or automatic notification is the only "communication" being made by the lawyer in this scenario—but such general contacts can hardly be considered to be on the subject of a "de-

---

127 *Polycast,* 129 F.R.D.at 625.

128 *Jenkins*, 956 F. Supp. at 696.

129 ABA Comm. on Prof'l Ethics & Responsibility, Formal Op. 95-396 (1995).

130 *See* MODEL RULES OF PROF'L CONDUCT R.4.2 cmt. 4 (2013); *see also* ABA Comm. on Prof'l Ethics & Responsibility, Formal Op. 95-396 (1995), ("[W]here the representation is general . . . the subject matter lacks sufficient specificity to trigger the operation of Rule 4.2.").

131 *See* CTR. FOR PROF'L RESPONSIBILITY, AM. BAR ASS'N, *supra* note 126, at 406–407, 409.

132 *See id.* at 409.

fined and specific" representation.[133] This conclusion is supported by the ABA's own analysis of this portion of the rule:

> For example, suppose a lawyer represents Defendant on a charge involving crime A. Under Rule 4.2, another lawyer may not, pursuant to a representation, either as prosecutor or as counsel for a co-defendant involving crime A, communicate with Defendant about that crime without leave of Defendant's lawyer. However, if the communicating lawyer represents a client with respect to a separate and distinct crime B and wishes to contact Defendant regarding that crime, the representation by counsel in crime A does not bar communications about crime B. Similarly, the fact that Defendant had been indicted on crime A would not prevent the prosecutor from communicating with Defendant . . . regarding crime B.[134]

Surely if this type of dialogue, which inevitably will include basic questions about the represented person's background, is considered to be "concerning matters outside the subject of the representation," then the social media activities at issue must also be similarly permissible.

Third, in the social media context, there is no real risk that the lawyer's legal skills and qualifications will give him or her an advantage over the represented layperson. Because the lawyer is, at most, triggering an automatically generated request for access or notification message, the lawyer's skill as an advocate and legal expertise simply do not come into play.

Fourth, unlike in a "real-world" interaction (face-to-face or over the phone) or personalized e-mail exchanges, the represented person is no more likely to disclose information via their social media accounts due to the social media connection by the lawyer. If anything, the represented person is *less* likely to disclose information, because of the lawyer's ability to access their social media sites. In the "real-world" scenarios contemplated by the rule, there are concerns that being directly confronted with an opposing lawyer may lead to confusion and intimidation that would result in the inadvertent disclosure of information by the represented person—in other words, the represented person might disclose information that they would not otherwise have chosen to share but for the questions of the lawyer. In the unique context of social media, where the lawyer merely has access to the represented person's sites but takes no steps to further engage in communication with the represented person,

---

133 *See* ABA Comm. on Prof'l Ethics & Responsibility, Formal Op. 95-396 (1995).
134 *Id.*

the only information disclosed is that which the represented person volunteers to share in this membership-based public forum—information that would have been shared regardless of the lawyer's ability to view it.[135]

Fifth, the social media activities at issue do not interfere with the represented person's relationship with their counsel. Social media users, including represented persons, decide what information to post and share on their websites and when to share it. A lawyer's request for access or notification message does not prompt the sharing of information, but rather simply informs the represented person that the lawyer wishes to view this information. Consequently, if in sharing information via social media, a represented person chooses to waive lawyer-client privilege, disregard advice of counsel, or make a statement without the benefit of their counsel's advice—that decision is made irrespective of the lawyer's social media activities. The lawyer's activities, therefore, cannot be considered a threat to the privilege or to the lawyer-client relationship. Further, once information is posted on the Internet, privilege is waived and the lawyer may properly obtain the information in any way outside of direct access (e.g., formal discovery, requesting a copy from a third party who already has access). Accordingly, the use of social media *by the represented person* is the real threat to the lawyer-client relationship and privilege, not use by opposing lawyers.

In sum, the purposes of Rule 4.2 are not offended by the lawyer's social media activities, because such activities do not seek to "elicit" information from a represented person, do not interfere with the lawyer-client relationship, and do not increase the likelihood that a represented person will disclose privileged or otherwise harmful information.[136] Such activities, therefore, fall within the realm of permissible ex parte communication that is not prohibited by Rule 4.2, as long as the lawyer

---

135 The ABA concludes that the prohibition of Rule 4.2 still applies even where the impermissible communication is initiated by the represented person. *See* ABA Comm. on Prof'l Ethics & Responsibility, *supra* note 123. Further, several courts have held that lawyers violated Rule 4.2 where the represented person initiated contact with the lawyer and the lawyer mostly just "listened to and took notes on the [represented person's] statement." *See, e.g.*, *In re* Howes, 940 P.2d 159, 166 (N.M. 1997); People v. Green, 274 N.W.2d 448 (Mich. 1979); Suarez v. State, 481 So.2d 1201 (Fla. 1985). However, these cases are distinguishable from the social media contacts at issue because in each case, the lawyer engaged in a personal and direct conversation with the represented person. *See In re Howes*, 940 P.2d at 163; *Green*, 274 N.W.2d at 451; *Suarez*, 481 So.2d at 1205. Even if the lawyer did not "overreach" by asking numerous questions, the "influence of the prosecutor's presence is immeasurable." *Green*, 274 N.W.2d at 456. In the social media context, the lawyer has no "presence" with which to intimidate or otherwise manipulate the represented person—the lawyer is just one member of a broad audience. Further, by posting social media information, the represented person is not "initiating communication" directly with the lawyer but rather making statements to a group of persons that includes the lawyer.

136 *See* MODEL RULES OF PROF'L CONDUCT R. 4.2 (2013).

refrains from going beyond simple requests for access or notifications, and is not actively engaging in a direct and personalized dialogue with the represented person.[137]

2. ABA Model Rule of Professional Conduct 4.3

Rule 4.3 of the ABA Model Rules of Professional Conduct states in relevant part as follows:

> In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer shall make reasonable efforts to correct the misunderstanding.[138]

The purpose of this portion of Rule 4.3 is fairly straightforward: to protect unrepresented persons from disclosing information that may be harmful to their interests because they have been misled by a lawyer, with an interest in a matter, to believe that the lawyer is disinterested in the matter.[139] This scenario is of particular concern because an unrepresented person, "particularly one not experienced in dealing with legal matters, might assume that a lawyer is disinterested in loyalties or is a disinterested authority on the law."[140] Further, the unrepresented person may believe that they can rely on the lawyer, as a neutral expert on the law, to provide them with legal advice and to protect their interests in the matter.

These concerns, however, are not implicated by the social media activities at issue here. First, the content of automatically generated requests for access and notification messages do not include any information specific to the lawyer, the unrepresented person, or the matter of particular interest to the lawyer. These requests and messages are uniformly produced by social media websites for all users who seek access to another user's site. There is no substantive interaction between the lawyer and the unrepresented person—the lawyer is not offering any information about him or herself to the unrepresented person. Consequently, in no way can the lawyer "state" or "imply" that he or she is disinterested in the matter; to "state" or "imply" requires the lawyer to make some sort of personalized statement.[141] In the social media context, the lawyer is not making a statement, but rather undertaking an action (seeking access to the unrepresented person's social media site).

---

137 *Id.* at cmt. 4.
138 MODEL RULES OF PROF'L CONDUCT R. 4.3 (2013).
139 *Id.*
140 *Id.* at cmt. 1.
141 *See* MODEL RULES OF PROF'L CONDUCT R. 4.3 (2013).

This interpretation of Rule 4.3 is borne out by case law. For example, one Louisiana federal court recently held that investigators who failed to identify themselves as working for an attorney when interviewing putative class members did not violate Rule 4.3 because they did not state or imply that they were disinterested, made no misrepresentations, and "did not deliberately foster any impression" that they were on the interviewees side.[142] In contrast, an Illinois federal court concluded that plaintiffs' attorneys violated Rule 4.3 by sending questionnaires to unrepresented employees of defendant, where the cover letter accompanying the questionnaire not only failed to state that the questionnaire was prepared for and distributed on behalf of the attorneys, but also contained misleading information designed to give the impression that the questionnaire was "neutral and unbiased."[143] Specifically, the letter described the questionnaire as an "independent survey" (implying there was no underlying motive in obtaining this information); stated that the employees' names were provided by a government agency (implying that the agency participated in or at least endorsed the survey); and explained that the questions were focused on two specific topics in order "to keep questions to an absolute minimum" (covering up the fact that these topics were the focus of the litigation).[144] As these cases demonstrate, in order to violate Rule 4.3 the lawyer must affirmatively offer information to the unrepresented person that causes them to believe that he or she is disinterested in the matter. The social media activities at issue pose no risk of this.

Second, as discussed extensively in the preceding section, the lawyer is not prompting the unrepresented person to share any information at all, let alone information specific to the matter or against the interests of the unrepresented person in that matter. Instead, the lawyer is simply seeking to view information the unrepresented person decides to post on whatever topic they choose—information that the unrepresented person would share regardless of the lawyer's access. Consequently, there is no need to fear that such social media activities could cause unrepresented people to disclose information harmful to their interests.

Third, similar to Rule 4.2, Rule 4.3 is motivated in part by a concern that a skilled attorney will take advantage of an unrepresented layperson. Again, because the sole "communication" between the lawyer and the unrepresented person is an automatically generated request for access or notification message, there is no danger that the lawyer's legal skills and qualifications will give the lawyer an advantage—practically or psychologically—over the unrepresented layperson. The lawyer's legal exper-

---

142 *In re* Katrina Canal Breaches Consol. Litig., No. 05-4182 "K" (2), 2008 WL 2066999, *6 (E.D. La. May 14, 2008) (internal quotation marks omitted).

143 *In re* Air Crash Disaster, 909 F. Supp. 1116, 1123 (N.D. Ill. 1995).

144 *Id.*

tise is immaterial and in no way influences the unrepresented person's decisions about what information to share and when to share it.

Fourth, since the lawyer is not communicating with the unrepresented person beyond the initial request or notification, it is impossible for the unrepresented person to believe that the lawyer is providing him with legal advice or advising him of his interests.

Consequently, lawyers seeking informal discovery of social media information do not violate Rule 4.3 as long as they limit their social media activities to initial requests for access or notification messages and take no affirmative action to mislead the unrepresented person into believing that they have no interest in the particular matter. Such activities honor the purposes of Rule 4.3 in that they do not "state" or "imply" that the lawyer is disinterested in the particular matter; do not instigate the sharing of information by the unrepresented person (contrary to their interests or otherwise); do not provide any opportunity for the lawyer to use his legal expertise to gain an advantage over the unrepresented person; and create no risk that the unrepresented person will mistakenly believe the lawyer is advising her of or otherwise protecting her interests in the matter.[145]

3. ABA Model Rule of Professional Conduct 8.4

Rule 8.4 of the ABA Model Rules of Professional Conduct states in relevant part: "It is professional misconduct for a lawyer to . . . (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation."[146] To a certain extent, the purpose of this rule is self-evident—to prevent lawyers from engaging in conduct involving dishonesty, fraud, deceit or misrepresentation. Rule 1.0(d) defines "fraud" as "conduct that is fraudulent under the substantive or procedural law of the applicable jurisdiction and has a purpose to deceive."[147] The Model Rules, however, do not provide specific definitions for "dishonesty," "deceit," or "misrepresentation," and authorities disagree about the distinctions between these terms and whether any or all of these terms require intent.[148] For example, one state's highest court has determined that fraud and deceit require "a false representation to another, with the intent that the other act upon the false representation to his or her damage" and that dishonesty involves "conduct indicating a disposition to lie, cheat or defraud," but that misrepresentation "need not be driven by an improper

145 *See* MODEL RULES OF PROF'L CONDUCT R. 4.3 (2013).

146 MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2013).

147 MODEL RULES OF PROF'L CONDUCT R. 1.0(d) (2013); *see also* CTR. FOR PROF'L RESPONSIBILITY, AM. BAR. ASS'N, *supra* note 126, § 8.4(c), at 613.

148 *See* CTR. FOR PROF'L RESPONSIBILITY, AM. BAR ASS'N, *supra* note 126, § 8.4(c), at 613–14.

motive. . . . [nor] does it require an intent to deceive or commit fraud."[149] In contrast, another court has concluded that "[dishonesty] includes conduct evincing a lack of honesty, probity, or integrity in principle," but does not necessarily involve conduct legally characterized as fraud, deceit, or misrepresentation.[150] At minimum, however, it appears that courts finding a violation of Rule 8.4(c) generally require some sort of culpable mental state, whether intent, purpose, or recklessness.[151]

Regardless of whether there is a culpable mental state requirement for Rule 8.4(c) violations, social media activities where the lawyer uses her true identity and profile to connect with a research target do not violate this rule. First, if the lawyer is able to gain access to the target's social media information using the lawyer's identity, there is no need (and no intent) to engage in affirmative dishonesty, deceit, fraud, or misrepresentation. Second, provided the lawyer takes no steps to hide her interest in the particular matter and connection to the client, failing to explicitly disclose this information when sending an automated request for access or notification message similarly does not constitute dishonesty, deceit, fraud, or misrepresentation. This point is most directly supported by the Philadelphia and New York City bar opinions. The former explicitly holds that although seeking access to social media information through a third party is a violation of Rule 8.4(c), the lawyer could seek such access herself, and that "would not be deceptive and would of course be permissible."[152] Further support of this interpretation is established by the fact that all but one of the remaining bar opinions do not even invoke Rule 8.4(c) as a justification for their constraints on social media usage, indicating that they consider this rule inapplicable in this scenario.[153] The San Diego Bar opinion alone concludes that failure to disclose the lawyer's interest in the matter constitutes a violation of Rule 8.4(c) because the "only way to gain access [to the target's social media information is] . . . for the attorney to exploit a party's unfamiliarity with the attorney's identity and therefore his adversarial relationship with the

---

149 *In re* Obert, 89 P.3d 1173, 1177–78 (Or. 2004) (internal quotation marks omitted). Several Oregon Supreme Court cases, including *In re Obert*, further note that misrepresentation can be "simply an omission of a fact that is knowing, false, and material in the sense that, had it been disclosed, the omitted fact would or could have influenced significantly the decision-making process." *Id.* at 1178, *see also In re* Eadie, 36 P.3d 468, 476, 333 Or. 42, 53 (Or. 2001); *In re* Gatti, 8 P.3d 966, 973, 330 Or. 517, 527–28 (Or. 2000). As far as can be determined, no other state embraces such a stringent standard for this rule—holding lawyers accountable for omissions of material fact absent a duty (e.g., to a client) or any intention to mislead.

150 *In re* Scanio, 919 A.2d 1137, 1143 (D.C. 2007) (internal quotation marks omitted).

151 *See* CTR. FOR PROF'L RESPONSIBILITY, AM. BAR ASS'N, *supra* note 126, § 8.4(c), at 614 (collecting cases).

152 Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11.

153 *Compare* N.Y.C. Bar Ass'n, *supra* note 23, *and* Phila. Bar Ass'n Prof'l Guidance Comm., *supra* note 11, *with* San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

recipient."[154] Critically, however, this conclusion fails to take into account the fact that social media information is information that is posted to the Internet. Consequently, the attorney has numerous ways to access this information, beyond seeking direct access (e.g., "friending" someone already connected to the target and asking them to provide a copy of all posts). Even more importantly, the target knows (or should know) that any information posted could conceivably be re-posted by others, end up anywhere on the Internet, and ultimately be seen by anyone. It is therefore simply inaccurate to paint basic social media activities as masterful deceptions employed to gain access to secret information.

An ABA opinion examining Rule 8.4(c) in an entirely different context lends further support to the contention that failure to disclose interest in a particular matter when engaging in these basic social media activities does not constitute dishonesty, deceit, fraud, or misrepresentation.[155] In this opinion, the ABA considers the question of whether a lawyer who provides legal assistance to a pro se litigant and helps the litigant prepare written submissions violates Rule 8.4(c), if the lawyer does not disclose or ensure the disclosure of the nature and extent of the assistance provided.[156] The ABA ultimately determines that such conduct does not violate Rule 8.4(c), explaining:

> [W]e do not believe that nondisclosure of the fact of legal assistance is dishonest so as to be prohibited by Rule 8.4(c). Whether it is dishonest for the lawyer to provide undisclosed assistance to a pro se litigant turns on whether the court would be misled by failure to disclose such assistance. The lawyer is making no statement at all to the forum regarding the nature or scope of the representation . . . . Absent an affirmative statement by the client, that can be attributed to the lawyer, that the documents were prepared without legal assistance, the lawyer has not been dishonest within the meaning of Rule 8.4(c).[157]

Although the scenario at issue in this opinion is far removed from the world of social media, the ABA's analysis sheds light on how Rule 8.4(c) is applied more broadly.[158] First, whether a failure to disclose information is considered "dishonest" within the meaning of Rule 8.4(c) depends on whether the other person or entity involved would be "mis-

---

154 San Diego Cnty. Bar Legal Ethics Comm., *supra* note 1.

155 ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 07-446 (2007).

156 *Id.*

157 *Id.*

158 *Id.*

led" by the failure to disclose.[159] Second, and most critically, a failure to disclose alone is not enough to constitute a Rule 8.4(c) violation—an "affirmative statement" that misleads the other party into believing something that is not true is also required.[160] In the social media context, the lawyer's failure to disclose the lawyer's interest in no way misleads the research target. The request for access or notification message from the lawyer contains the exact same information as those sent by any other social media user, and the target has no less reason to suspect the lawyer of having adverse interests than any other user. Further, these automatically generated messages contain no affirmative statements designed to lure the target into granting access or believing that the lawyer does *not* have adverse interests.

In sum, there is simply no way to construe the basic social media activities at issue here as "conduct involving dishonesty, fraud, deceit or misrepresentation."[161] Where the lawyer seeking social media information uses his or her true identity and real social media profiles in requests for access and notification messages and takes no steps to hide his or her interests in a particular matter, there is no Rule 8.4(c) violation.[162]

CONCLUSION

Contrary to the prevailing view according to state and local bars and practitioners, a close examination of the most relevant rules of professional conduct suggests that informal discovery of social media information is broadly permissible, limited only by prohibitions on outright fraud and deception. As long as lawyers refrain from contact beyond the initial requests for access and notification messages and rely on only their true identities and real social media profiles, it appears that informal discovery of social media information is well within the bounds of these ethical rules.

Despite the strength of this argument, however, in light of the fairly restrictive opinions issued by state and local bars thus far, practicing lawyers have taken a conservative approach to this type of informal discovery rather than risk the violation of ethical rules. Such caution is particularly understandable and advisable, considering that the few existing opinions do not provide consistent rulings and there is a serious lack of clarity regarding the limits of permissible conduct in this area. The unfortunate result of this scant and confusing guidance has been a severe chilling effect on the use of this critical resource by lawyers—an

159 *Id.*
160 *Id.*
161 *See* MODEL RULES OF PROF'L CONDUCT R. 8.4(c) (2013).
162 *Id.*

outcome that is increasingly impracticable as the prevalence and importance of social media in our society and culture continues to grow.

We, therefore, urge the ABA, state bars, and other committees to undertake a careful and informed study of the nature and functionality of social media as a new and distinct method of producing and sharing information and, further, to clarify that the informal discovery of social media is broadly permissible under the existing rules of professional conduct. With fuller knowledge and understanding of social media, the ABA and state bars will be better able to balance the prolificacy, pervasiveness, and usefulness of this type of information against the purposes and protections established by the rules of professional conduct. This will allow them to provide instructive guidance that can reverse the chilling effect the handful of existing opinions has created. Further, by explicitly addressing the complex nature of social media information and expressly permitting broad informal discovery of this information, such guidance would provide much-needed clarity to lawyers now and in the future, as social media platforms and applications continue to rapidly evolve and grow.

2018 WL 828101

THIS DECISION IS UNCORRECTED AND SUBJECT TO REVISION BEFORE PUBLICATION IN THE NEW YORK REPORTS.

Court of Appeals of New York.

Kelly FORMAN, Respondent,
v.
Mark HENKIN, Appellant.

No. 1
|
Decided February 13, 2018

Synopsis

Background: Horseback rider, who fell from horse and allegedly suffered spinal and traumatic brain injuries, brought personal injury action against owner of horse. The Supreme Court, New York County, Lucy Billings, J., 2014 WL 1162201, granted owner's motion to compel discovery with respect to rider's private posts, including photographs, on social networking website. Rider appealed. The Supreme Court, Appellate Division, 134 A.D.3d 529, 22 N.Y.S.3d 178, affirmed as modified. Owner appealed.

Holdings: The Court of Appeals, DiFiore, Chief Judge, held that:

[1] pre-accident and post-accident photographs privately posted on rider's social networking website account were discoverable, and

[2] data revealing timing and number of characters in post-accident messages privately posted on rider's account was discoverable.

Reversed.

West Headnotes (25)

[1] **Appeal and Error**
Scope of Inquiry

A review of a Supreme Court, Appellate Division order by the Court of Appeals is limited to those parts of the order that have been appealed and that aggrieve the appealing party.

Cases that cite this headnote

[2] **Pretrial Procedure**
Relevancy and materiality

A party seeking discovery must satisfy the threshold requirement that the request is reasonably calculated to yield information that is material and necessary, i.e., relevant, regardless of whether discovery is sought from another party or a nonparty. N.Y. CPLR §§ 3101(a)(1), 3101(a)(4).

Cases that cite this headnote

[3] **Pretrial Procedure**
Discovering truth, narrowing issues, and eliminating surprise

Pretrial Procedure
Liberality in allowance of remedy

The statute governing the scope of discovery embodies the policy determination that liberal discovery encourages fair and effective resolution of disputes on the merits, minimizing the possibility for ambush and unfair surprise. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[4] **Pretrial Procedure**
Scope of Discovery

The right to disclosure under the statute governing the scope of discovery, although broad, is not unlimited. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[5] **Pretrial Procedure**
Work-product privilege

Privileged Communications and Confidentiality

Privileged Communications and Confidentiality

The rule governing the scope of discovery establishes three categories of protected materials, also supported by policy considerations: privileged matter, which is absolutely immune from discovery; attorney's work product, which is also absolutely immune; and trial preparation materials, which are subject to disclosure only on a showing of substantial need and undue hardship. N.Y. CPLR §§ 3101(b), 3101(c), 3101(d).

Cases that cite this headnote

[6] **Pretrial Procedure**
Objections and protective orders

Privileged Communications and Confidentiality
Construction in general

Privileged Communications and Confidentiality
Presumptions and burden of proof

The burden of establishing a right to protection from disclosure under the privileged matter, attorney work product, and trial preparation materials provisions of the rule governing the scope of discovery is with the party asserting it; the protection claimed must be narrowly construed, and its application must be consistent with the purposes underlying the immunity. N.Y. CPLR §§ 3101(b), 3101(c), 3101(d).

Cases that cite this headnote

[7] **Pretrial Procedure**
Control by court in general

Pretrial Procedure
Scope of Discovery

When resolving a discovery dispute, competing interests must always be balanced, and the need for discovery must be weighed against any special burden to be borne by the opposing party. N.Y. CPLR §§ 3101, 3103(a).

Cases that cite this headnote

[8] **Pretrial Procedure**
Control by court in general

Pretrial Procedure
Scope of Discovery

When a court is called upon to resolve a discovery dispute, discovery requests must be evaluated on a case-by-case basis with due regard for the strong policy supporting open disclosure.

Cases that cite this headnote

[9] **Pretrial Procedure**
Control by court in general

While the courts have the authority to oversee disclosure during discovery, by design, the process often can be managed by the parties without judicial intervention.

Cases that cite this headnote

[10] **Attorney and Client**
Nature and term of office

Attorneys, while functioning as advocates for their clients' interests, are also officers of the court who are expected to make a bona fide effort to properly meet their obligations in the disclosure process during discovery.

Cases that cite this headnote

[11] **Appeal and Error**
Depositions, affidavits, or discovery

Absent an error of law or an abuse of discretion, the Court of Appeals will not disturb a determination resolving a discovery dispute.

Cases that cite this headnote

[12] **Appeal and Error**
Power to Review

Appeal and Error
Abuse of discretion

The Appellate Division has the power to exercise independent discretion, that is, to substitute its discretion for that of the trial court, even when it concludes the trial court's order was merely improvident and not an abuse of discretion, and when it does so applying the proper legal principles, the Court of Appeals will review the resulting Appellate Division order under the deferential abuse of discretion standard.

Cases that cite this headnote

[13] **Pretrial Procedure**
Relevancy and materiality

New York discovery rules do not condition a party's receipt of disclosure on a showing that the items the party seeks actually exist; rather, the request need only be appropriately tailored and reasonably calculated to yield relevant information. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[14] **Pretrial Procedure**
Relevancy and materiality

The purpose of discovery is to determine if material relevant to a claim or defense exists; in many if not most instances, a party seeking disclosure will not be able to demonstrate that items it has not yet obtained contain material evidence. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[15] **Pretrial Procedure**
Documents, papers, and books in general

An account holder's privacy settings do not govern the scope of disclosure of materials posted on a social networking website. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[16] **Pretrial Procedure**
Documents, papers, and books in general

The commencement of a personal injury action does not render a party's entire social networking website account automatically discoverable. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[17] **Pretrial Procedure**
Scope of Discovery

Even under New York's broad disclosure paradigm, litigants are protected from unnecessarily onerous application of the discovery statutes.

Cases that cite this headnote

[18] **Pretrial Procedure**
Determination

A court addressing a dispute over the scope of discovery of materials on a social networking website should first consider the nature of the event giving rise to the litigation and the injuries claimed, as well as any other information specific to the case, to assess whether relevant material is likely to be found on the social networking website account. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[19] **Pretrial Procedure**
Determination

Pretrial Procedure
Order

A court addressing a dispute over the scope of discovery of materials on a social networking website should balance the potential utility of the information sought against any specific privacy or other concerns raised by the account holder, and the court should issue an order tailored to the particular controversy that identifies the types of materials that must be disclosed while avoiding disclosure of nonrelevant materials. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[20] **Pretrial Procedure**
Determination

In resolving a discovery dispute over material on a social networking website in a personal injury case, it is appropriate for the court to consider the nature of the underlying incident and the injuries claimed and to craft a rule for discovering information specific to each. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[21] **Pretrial Procedure**
Relevancy and materiality

Private materials may be subject to discovery if they are relevant. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[22] **Privileged Communications and Confidentiality**
Acts constituting waiver

When a party commences an action, affirmatively placing a mental or physical condition in issue, certain privacy interests relating to relevant medical records, including the physician-patient privilege, are waived. N.Y. CPLR § 4504.

Cases that cite this headnote

[23] **Pretrial Procedure**
Relevancy and materiality

For purposes of disclosure during discovery, the threshold inquiry is not whether the materials sought are private but whether they are reasonably calculated to contain relevant information. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[24] **Pretrial Procedure**
Photographs;X rays;sound recordings

Pre-accident photographs privately posted on horseback rider's social networking website account that she intended to introduce at trial and all privately posted post-accident photographs of rider that did not depict nudity or romantic encounters were discoverable, in personal injury action by rider, who fell from horse and allegedly suffered spinal and traumatic brain injuries, against owner of horse, even if only publicly-available photograph on account was not relevant, since rider had tendency to privately post photographs that were representative of her activities, and subject photographs were relevant to rider's assertions that she could no longer engage in pre-accident activities she had enjoyed and that she had become reclusive. N.Y. CPLR § 3101(a).

Cases that cite this headnote

[25] **Pretrial Procedure**
Relevancy and materiality

Data revealing timing and number of characters in post-accident messages privately posted on horseback rider's social networking website account was discoverable, in personal injury action against owner of horse by rider, who fell from horse and allegedly suffered spinal and traumatic brain injuries, since such data was relevant to rider's claim that she suffered cognitive injuries that caused her to have difficulty writing and using a computer, particularly her claim that she was painstakingly slow in crafting messages. N.Y. CPLR § 3101(a).

Cases that cite this headnote

Attorneys and Law Firms

Michael A. Bono, for appellant.

Kenneth J. Gorman, for respondent.

Defense Association of New York, Inc., amicus curiae.

Opinion

OPINION

DIFIORE, Chief Judge:

*1 In this personal injury action, we are asked to resolve a dispute concerning disclosure of materials from plaintiff's **Facebook** account.

Plaintiff alleges that she was injured when she fell from a horse owned by defendant, suffering spinal and traumatic brain injuries resulting in cognitive deficits, memory loss, difficulties with written and oral communication, and social isolation. At her deposition, plaintiff stated that she previously had a **Facebook** account on which she posted "a lot" of photographs showing her pre-accident active lifestyle but that she deactivated the account about six months after the accident and could not recall whether any post-accident photographs were posted. She maintained that she had become reclusive as a result of her injuries and also had difficulty using a computer and composing coherent messages. In that regard, plaintiff produced a document she wrote that contained misspelled words and faulty grammar in which she represented that she could no longer express herself the way she did before the accident. She contended, in particular, that a simple email could take hours to write because she had to go over written material several times to make sure it made sense.

Defendant sought an unlimited authorization to obtain plaintiff's entire "private" **Facebook** account, contending the photographs and written postings would be material and necessary to his defense of the action under CPLR 3101(a). When plaintiff failed to provide the authorization (among other outstanding discovery), defendant moved to compel, asserting that the **Facebook** material sought was relevant to the scope of plaintiff's injuries and her credibility. In support of the motion, defendant noted that plaintiff alleged that she was quite active before the accident and had posted photographs on **Facebook** reflective of that fact, thus affording a basis to conclude her **Facebook** account would contain evidence relating to her activities. Specifically, defendant cited the claims that plaintiff can no longer cook, travel, participate in sports, horseback ride, go to the movies, attend the theater, or go boating, contending that photographs and messages she posted on **Facebook** would likely be material to these allegations and her claim that the accident negatively impacted her ability to read, write, word-find, reason and use a computer.

Plaintiff opposed the motion arguing, as relevant here, that defendant failed to establish a basis for access to the "private" portion of her **Facebook** account because, among other things, the "public" portion contained only a single photograph that did not contradict plaintiff's claims or deposition testimony. Plaintiff's counsel did not affirm that she had reviewed plaintiff's **Facebook** account, nor allege that any specific material located therein, although potentially relevant, was privileged or should be shielded from disclosure on privacy grounds. At oral argument on the motion, defendant reiterated that the **Facebook** material was reasonably likely to provide evidence relevant to plaintiff's credibility, noting for example that the timestamps on **Facebook** messages would reveal the amount of time it takes plaintiff to write a post or respond to a message. Supreme Court inquired whether there is a way to produce data showing the timing and frequency of messages without revealing their contents and defendant acknowledged that it would be possible for plaintiff to turn over data of that type, although he continued to seek the content of messages she posted on **Facebook**.

*2 Supreme Court granted the motion to compel to the limited extent of directing plaintiff to produce all photographs of herself privately posted on **Facebook** prior to the accident that she intends to introduce at trial, all photographs of herself privately posted on **Facebook** after the accident that do not depict nudity or romantic encounters, and an authorization for **Facebook** records showing each time plaintiff posted a private message after the accident and the number of characters or words in the messages. Supreme Court did not order disclosure of the content of any of plaintiff's written **Facebook** posts, whether authored before or after the accident.

[1] Although defendant was denied much of the disclosure sought in the motion to compel, only plaintiff appealed to the Appellate Division.[1] On that appeal, the court modified by limiting disclosure to photographs posted on **Facebook** that plaintiff intended to introduce at trial (whether pre– or post-accident) and eliminating the authorization permitting defendant to obtain data relating to post-accident messages, and otherwise affirmed. Two Justices dissented, concluding defendant was entitled to broader access to plaintiff's **Facebook** account and calling for reconsideration of that court's recent precedent addressing disclosure of social media information as unduly restrictive and inconsistent with New York's policy of open discovery. The Appellate Division granted defendant leave to appeal to this Court, asking whether its

order was properly made. We reverse, reinstate Supreme Court's order and answer that question in the negative.

[2] [3] Disclosure in civil actions is generally governed by CPLR 3101(a), which directs: "[t]here shall be full disclosure of all matter material and necessary to the prosecution or defense of an action, regardless of the burden of proof." We have emphasized that "[t]he words 'material and necessary,' ... are to be interpreted liberally to require disclosure, upon request, of any facts bearing on the controversy which will assist preparation for trial by sharpening the issues and reducing delay and prolixity. The test is one of usefulness and reason" (*Allen v. Crowell–Collier Publ. Co.*, 21 N.Y.2d 403, 406, 288 N.Y.S.2d 449, 235 N.E.2d 430 [1968]; *see also Andon v. 302–304 Mott St. Assoc.*, 94 N.Y.2d 740, 746, 709 N.Y.S.2d 873, 731 N.E.2d 589 [2000]). A party seeking discovery must satisfy the threshold requirement that the request is reasonably calculated to yield information that is "material and necessary"—i.e., relevant—regardless of whether discovery is sought from another party (*see* CPLR 3101[a][1]) or a nonparty (CPLR 3101[a][4]; *see e.g. Matter of Kapon v. Koch*, 23 N.Y.3d 32, 988 N.Y.S.2d 559, 11 N.E.3d 709 [2014]). The "statute embodies the policy determination that liberal discovery encourages fair and effective resolution of disputes on the merits, minimizing the possibility for ambush and unfair surprise" (*Spectrum Systems Intern. Corp. v. Chemical Bank*, 78 N.Y.2d 371, 376, 575 N.Y.S.2d 809, 581 N.E.2d 1055 [1991]).

[4] [5] [6] The right to disclosure, although broad, is not unlimited. CPLR 3101 itself "establishes three categories of protected materials, also supported by policy considerations: privileged matter, absolutely immune from discovery (CPLR 3101[b]); attorney's work product, also absolutely immune (CPLR 3101[c]); and trial preparation materials, which are subject to disclosure only on a showing of substantial need and undue hardship" (*Spectrum*, *supra*, at 377, 575 N.Y.S.2d 809, 581 N.E.2d 1055). The burden of establishing a right to protection under these provisions is with the party asserting it—"the protection claimed must be narrowly construed; and its application must be consistent with the purposes underlying the immunity" (*id.*).

*3 [7] [8] [9] [10] [11] [12] In addition to these restrictions, this Court has recognized that "litigants are not without protection against unnecessarily onerous application of the disclosure statutes. Under our discovery statutes and case law competing interests must always be balanced; the need for discovery must be weighed against any special burden to be borne by the opposing party" (*Kavanagh v. Ogden Allied Maintenance Corp.*, 92 N.Y.2d 952, 954, 683 N.Y.S.2d 156, 705 N.E.2d 1197 [1998] [citations and internal quotation marks omitted]; *see* CPLR 3103[a]). Thus, when courts are called upon to resolve a dispute,[2] discovery requests "must be evaluated on a case-by-case basis with due regard for the strong policy supporting open disclosure ... Absent an [error of law or an] abuse of discretion, this Court will not disturb such a determination (*Andon*, *supra*, 94 N.Y.2d at 747, 709 N.Y.S.2d 873, 731 N.E.2d 589; *see Kavanagh*, *supra*, 92 N.Y.2d at 954, 683 N.Y.S.2d 156, 705 N.E.2d 1197).[3]

Here, we apply these general principles in the context of a dispute over disclosure of social media materials. **Facebook** is a social networking website "where people can share information about their personal lives, including posting photographs and sharing information about what they are doing or thinking" (*Romano v. Steelcase, Inc.*, 30 Misc.3d 426, 907 N.Y.S.2d 650 [Sup. Ct. Suffolk County 2010]). Users create unique personal profiles, make connections with new and old "friends" and may "set privacy levels to control with whom they share their information" (*id.*). Portions of an account that are "public" can be accessed by anyone, regardless of whether the viewer has been accepted as a "friend" by the account holder—in fact, the viewer need not even be a fellow **Facebook** account holder (*see* **Facebook** Help: What audiences can I choose from when I share? https://www.facebook.com/help/211513702214269?helpref=faq_content [last accessed January 15, 2018]). However, if portions of an account are "private," this typically means that items are shared only with "friends" or a subset of "friends" identified by the account holder (*id.*). While **Facebook**—and sites like it—offer relatively new means of sharing information with others, there is nothing so novel about **Facebook** materials that precludes application of New York's long-standing disclosure rules to resolve this dispute.

*4 On appeal in this Court, invoking New York's history of liberal discovery, defendant argues that the Appellate Division erred in employing a heightened threshold for production of social media records that depends on what the account holder has chosen to share on the public portion of the account. We agree. Although it is unclear

precisely what standard the Appellate Division applied, it cited its prior decision in *Tapp v. New York State Urban Dev. Corp.*, 102 A.D.3d 620, 958 N.Y.S.2d 392 [1st Dept. 2013]), which stated: "To warrant discovery, defendants must establish a factual predicate for their request *by identifying relevant information in plaintiff's* ***Facebook*** *account*—that is, information that 'contradicts or conflicts with plaintiff's alleged restrictions, disabilities, and losses, and other claims' " (*id.* at 620, 958 N.Y.S.2d 392 [emphasis added]). Several courts applying this rule appear to have conditioned discovery of material on the "private" portion of a **Facebook** account on whether the party seeking disclosure demonstrated there was material in the "public" portion that tended to contradict the injured party's allegations in some respect (*see e.g. Spearin v. Linmar*, 129 A.D.3d 528, 11 N.Y.S.3d 156 [1st Dept. 2015]; *Nieves v. 30 Ellwood Realty LLC*, 39 Misc.3d 63, 966 N.Y.S.2d 808 [App. Term. 2013]; *Pereira v. City of New York*, 40 Misc.3d 1210[A], 2013 WL 3497615 [Sup. Ct. Queens County 2013]; *Romano*, *supra*, 30 Misc.3d 426, 907 N.Y.S.2d 650). Plaintiff invoked this precedent when arguing, in opposition to the motion to compel, that defendant failed to meet the minimum threshold permitting discovery of any **Facebook** materials.

Before discovery has occurred—and unless the parties are already **Facebook** "friends"—the party seeking disclosure may view only the materials the account holder happens to have posted on the public portion of the account. Thus, a threshold rule requiring that party to "identify relevant information in [the] **Facebook** account" effectively permits disclosure only in limited circumstances, allowing the account holder to unilaterally obstruct disclosure merely by manipulating "privacy" settings or curating the materials on the public portion of the account.[4] Under such an approach, disclosure turns on the extent to which some of the information sought is already accessible—and not, as it should, on whether it is "material and necessary to the prosecution or defense of an action" (*see* CPLR 3101[a]).

[13] **[14]** **[15]** New York discovery rules do not condition a party's receipt of disclosure on a showing that the items the party seeks actually exist; rather, the request need only be appropriately tailored and reasonably calculated to yield relevant information. Indeed, as the name suggests, the purpose of discovery is to determine if material relevant to a claim or defense exists. In many if not most instances, a party seeking disclosure will not be able to demonstrate that items it has not yet obtained contain material evidence. Thus, we reject the notion that the account holder's so-called "privacy" settings govern the scope of disclosure of social media materials.

[16] **[17]** That being said, we agree with other courts that have rejected the notion that commencement of a personal injury action renders a party's entire **Facebook** account automatically discoverable (*see e.g. Kregg v. Maldonado*, 98 A.D.3d 1289, 1290, 951 N.Y.S.2d 301 [4th Dept. 2012] [rejecting motion to compel disclosure of all social media accounts involving injured party without prejudice to narrowly-tailored request seeking only relevant information]; *Giacchetto*, *supra*, 293 F.R.D. 112, 115; *Kennedy v. Contract Pharmacal Corp.*, 2013 WL 1966219, *2 [E.D.N.Y. 2013]). Directing disclosure of a party's entire **Facebook** account is comparable to ordering discovery of every photograph or communication that party shared with any person on any topic prior to or since the incident giving rise to litigation—such an order would be likely to yield far more nonrelevant than relevant information. Even under our broad disclosure paradigm, litigants are protected from "unnecessarily onerous application of the discovery statutes" (*Kavanagh*, *supra*, 92 N.Y.2d at 954, 683 N.Y.S.2d 156, 705 N.E.2d 1197).

***5** **[18]** **[19]** **[20]** Rather than applying a one-size-fits-all rule at either of these extremes, courts addressing disputes over the scope of social media discovery should employ our well-established rules—there is no need for a specialized or heightened factual predicate to avoid improper "fishing expeditions." In the event that judicial intervention becomes necessary, courts should first consider the nature of the event giving rise to the litigation and the injuries claimed, as well as any other information specific to the case, to assess whether relevant material is likely to be found on the **Facebook** account. Second, balancing the potential utility of the information sought against any specific "privacy" or other concerns raised by the account holder, the court should issue an order tailored to the particular controversy that identifies the types of materials that must be disclosed while avoiding disclosure of nonrelevant materials. In a personal injury case such as this it is appropriate to consider the nature of the underlying incident and the injuries claimed and to craft a rule for discovering information specific to each. Temporal limitations may also be appropriate—for example, the court should

consider whether photographs or messages posted years before an accident are likely to be germane to the litigation. Moreover, to the extent the account may contain sensitive or embarrassing materials of marginal relevance, the account holder can seek protection from the court (*see* CPLR 3103[a]). Here, for example, Supreme Court exempted from disclosure any photographs of plaintiff depicting nudity or romantic encounters.

[21] [22] [23] Plaintiff suggests that disclosure of social media materials necessarily constitutes an unjustified invasion of privacy. We assume for purposes of resolving the narrow issue before us that some materials on a **Facebook** account may fairly be characterized as private. [5] But even private materials may be subject to discovery if they are relevant. For example, medical records enjoy protection in many contexts under the physician-patient privilege (*see* CPLR 4504). But when a party commences an action, affirmatively placing a mental or physical condition in issue, certain privacy interests relating to relevant medical records—including the physician-patient privilege—are waived (*see Arons v. Jutkowitz*, 9 N.Y.3d 393, 409, 850 N.Y.S.2d 345, 880 N.E.2d 831 [2007]; *Dillenbeck v. Hess*, 73 N.Y.2d 278, 287, 539 N.Y.S.2d 707, 536 N.E.2d 1126 [1989]). For purposes of disclosure, the threshold inquiry is not whether the materials sought are private but whether they are reasonably calculated to contain relevant information.

[24] Applying these principles here, the Appellate Division erred in modifying Supreme Court's order to further restrict disclosure of plaintiff's **Facebook** account, limiting discovery to only those photographs plaintiff intended to introduce at trial. [6] With respect to the items Supreme Court ordered to be disclosed (the only portion of the discovery request we may consider), defendant more than met his threshold burden of showing that plaintiff's **Facebook** account was reasonably likely to yield relevant evidence. At her deposition, plaintiff indicated that, during the period prior to the accident, she posted "a lot" of photographs showing her active lifestyle. Likewise, given plaintiff's acknowledged tendency to post photographs representative of her activities on **Facebook**, there was a basis to infer that photographs she posted after the accident might be reflective of her post-accident activities and/or limitations. The request for these photographs was reasonably calculated to yield evidence relevant to plaintiff's assertion that she could no longer engage in the activities she enjoyed before the accident and that she had become reclusive. It happens in this case that the order was naturally limited in temporal scope because plaintiff deactivated her **Facebook** account six months after the accident and Supreme Court further exercised its discretion to exclude photographs showing nudity or romantic encounters, if any, presumably to avoid undue embarrassment or invasion of privacy.

*6 [25] In addition, it was reasonably likely that the data revealing the timing and number of characters in posted messages would be relevant to plaintiffs' claim that she suffered cognitive injuries that caused her to have difficulty writing and using the computer, particularly her claim that she is painstakingly slow in crafting messages. Because Supreme Court provided defendant no access to the content of any messages on the **Facebook** account (an aspect of the order we cannot review given defendant's failure to appeal to the Appellate Division), we have no occasion to further address whether defendant made a showing sufficient to obtain disclosure of such content and, if so, how the order could have been tailored, in light of the facts and circumstances of this case, to avoid discovery of nonrelevant materials. [7]

In sum, the Appellate Division erred in concluding that defendant had not met his threshold burden of showing that the materials from plaintiff's **Facebook** account that were ordered to be disclosed pursuant to Supreme Court's order were reasonably calculated to contain evidence "material and necessary" to the litigation. A remittal is not necessary here because, in opposition to the motion, plaintiff neither made a claim of statutory privilege, nor offered any other specific reason—beyond the general assertion that defendant did not meet his threshold burden —why any of those materials should be shielded from disclosure.

Accordingly, the Appellate Division order insofar as appealed from should be reversed, with costs, the Supreme Court order reinstated and the certified question answered in the negative.

Order insofar as appealed from reversed, with costs, order of Supreme Court, New York County, reinstated and certified question answered in the negative.

Judges Rivera, Stein, Fahey, Garcia, Wilson and Feinman concur.

All Citations

--- N.E.3d ----, 2018 WL 828101, 2018 N.Y. Slip Op. 01015

Footnotes

1 Defendant's failure to appeal Supreme Court's order impacts the scope of his appeal in this Court. "Our review of [an] Appellate Division order is 'limited to those parts of the [order] that have been appealed and that aggrieve the appealing party' " (*Hain v. Jamison*, 28 N.Y.3d 524, 534, 46 N.Y.S.3d 502, 68 N.E.3d 1233 [2016], quoting *Hecht v. City of New York*, 60 N.Y.2d 57, 467 N.Y.S.2d 187, 454 N.E.2d 527 [1983]). Because defendant did not cross-appeal and, thus, sought no affirmative relief from the Appellate Division, he is aggrieved by the Appellate Division order only to the extent it further limited Supreme Court's disclosure order.

2 While courts have the authority to oversee disclosure, by design the process often can be managed by the parties without judicial intervention. If the party seeking disclosure makes a targeted demand for relevant, non-privileged materials (*see* CPLR 3120[1][i], [2] [permitting a demand for items within the other party's "possession, custody or control," which "shall describe each item and category with reasonable particularity"]), counsel for the responding party—after examining any potentially responsive materials—should be able to identify and turn over items complying with the demand. Attorneys, while functioning as advocates for their clients' interests, are also officers of the court who are expected to make a bona fide effort to properly meet their obligations in the disclosure process. When the process is functioning as it should, there is little need for a court in the first instance to winnow the demand or exercise its in camera review power to cull through the universe of potentially responsive materials to determine which are subject to discovery.

3 Further, the Appellate Division has the power to exercise independent discretion—to substitute its discretion for that of Supreme Court, even when it concludes Supreme Court's order was merely improvident and not an abuse of discretion—and when it does so applying the proper legal principles, this Court will review the resulting Appellate Division order under the deferential "abuse of discretion" standard (*see e.g. Andon*, *supra*; *Kavanagh*, *supra*; *see generally Kapon*, *supra*).

4 This rule has been appropriately criticized by other courts. As one federal court explained, "[t]his approach can lead to results that are both too broad and too narrow. On the one hand, a plaintiff should not be required to turn over the private section of his or her **Facebook** profile (which may or may not contain relevant information) merely because the public section undermines the plaintiff's claims. On the other hand, a plaintiff should be required to review the private section and produce any relevant information, regardless of what is reflected in the public section ... Furthermore, this approach shields from discovery the information of **Facebook** users who do not share any information publicly" (*Giacchetto v. Patchogue–Medford Union Free School Dist.*, 293 F.R.D. 112, 114 [E.D.N.Y. 2013]).

5 There is significant controversy on that question. Views range from the position taken by plaintiff that anything shielded by privacy settings is private, to the position taken by one commentator that "anything contained in a social media website is not 'private' ... [S]ocial media exists to facilitate social behavior and is not intended to serve as a personal journal shielded from others or a database for storing thoughts and photos" (McPeak, The **Facebook** Digital Footprint: Paving Fair and Consistent Pathways to Civil Discovery or Social Media Data, 48 Wake Forest L Rev 887, 929 [2013]).

6 Because plaintiff would be unlikely to offer at trial any photographs tending to contradict her claimed injuries or her version of the facts surrounding the accident, by limiting disclosure in this fashion the Appellate Division effectively denied disclosure of any evidence potentially relevant to the defense. To the extent the order may also contravene CPLR 3101(i), we note that neither party cited that provision in Supreme Court and we therefore have no occasion to further address its applicability, if any, to this dispute.

7 At oral argument, Supreme Court indicated that, depending on what the data ordered to be disclosed revealed concerning the frequency of plaintiff's post-accident messages, defendant could possibly pursue a follow-up request for disclosure of the content. We express no views with respect to any such future application.

End of Document

The Ethics of Working with the I.P., P.I.

By Brian S. Faughnan

Long ago, Francis Bacon wrote "knowledge is power." Albert Einstein much more recently said that "information is not knowledge." Yet, transitive properties of equality and inequality notwithstanding, I find it difficult to imagine that either of those two great thinkers in history would argue my conclusion that, in today's world, information is power. Information can be a potent weapon for lawyers generally, litigators particularly, and lawyers handling intellectual property matters especially. Not surprisingly, some people will go to great lengths to try to shield information they do not want others to access, and other people will go to great lengths to try to acquire information others have shielded. Intellectual property lawyers (and often their clients as well) are often both kinds of people.

Such lawyers are often engaged in the art of investigation. The ability of lawyers to seek out and acquire information, or to shield and protect it for that matter, is not just constrained by what is illegal, but also by the rules of ethics that govern our profession. Given that those rules place such importance upon honesty, trustworthiness, and candor, there lurks an obvious, but highly important, question for *Landslide*® magazine readers: Do the ethics rules governing lawyers leave any room for lawyers to be involved in the use of deceptive investigative tactics, including certain types of pretexting activity?

Before plowing forward, it seems advisable to ensure that my reference to "pretexting" is clear. After all, it was but a few years ago that the high profile HP scandal introduced the term "pretexting" to many who may have never heard of it before. While "pretexting" is often carelessly used to mean only certain types of inquiries, like the pretexting for telephone records at the heart of the HP scandal (and that has been a federal crime since Congress passed the Telephone Records and Privacy Protection Act of 2006[1] in direct response to that scandal), the term actually encompasses a much broader array of activities.

"Pretexting" can correctly be used to describe any type of activity in which a person undertakes to gather information by putting forth an outward appearance as to his or her intentions or identity that is false. Some such activities are expressly made unlawful by statute based on the information targeted, like pretexting for phone records is now under federal law and like pretexting for financial records has been since the passage of Gramm-Leach-Bliley in 1999. Yet, there are an infinite number of other deceptive actions that might be employed as an investigative tactic that are not obviously illegal. For example, something as seemingly innocuous as a lawyer visiting her client's competitor's storefront to purchase a product for the purpose of confirming her client's suspicions about infringing activity before filing suit is fairly classified as pretexting activity if the lawyer does not let the competitor know who she is and why she is there.

Not surprisingly, there are examples of lawyers, or others at their behest, using deceptive tactics to further ends that many would agree justify such means. Otherwise legal conduct properly categorized as pretexting historically has been particularly effective at rooting out racial and other forms of insidious discrimination through the use of "testers"—people sent to pretend, for example, to be potential renters or consumers in order to determine whether a person or entity is engaged in discriminatory practices.[2] If these ends justify the means, a number of questions may flow more or less naturally, including shouldn't lawyer deception in the name of protecting intellectual property rights also be deemed acceptable conduct? Yet, at some point, every reader will begin to notice the slipperiness of the slope. After all, wouldn't being able to trick a wrongdoer into letting his guard down and revealing information he might otherwise try to shield be a useful thing for almost any lawyer, pursuing almost any type of case, to have in his arsenal? In the face of such questions, it is an ideal time to discuss the ethical restrictions that matter for lawyers wrestling with whether they can participate in an investigation involving deceptive tactics such as pretexting.

Using the ABA Model Rules as our guide (for the convenience of not getting bogged down in a discussion of state-based variations on the Rules, if for no other reason), six ethics rules are implicated, and potentially transgressed, when a lawyer either engages in deceptive conduct in connection with undertaking an investigation or oversees the investigative efforts of nonlawyers using deceptive conduct. For better compartmentalization, I have grouped those ethics rules into two buckets: (1) those relating to the "how" of the investigation, and (2) those relating to the "who" of the investigation.

There are three rules in our "how" bucket: Model Rules 4.1(a), 4.4(a), and 8.4(c). Rule 4.1(a) prohibits a lawyer "[i]n the course of representing a client" from "knowingly mak[ing] a false statement of material fact or law to a third person." Rule 8.4(c) goes even further by declaring it to be unethical for a lawyer to "engage in conduct involving dishonesty, fraud, deceit or misrepresentation." Notably, this ethical prohibition is not limited to circumstances when a lawyer is representing a client, does not explicitly impose any requirement of knowledge on the lawyer's part, and does not limit its restriction to "material" statements. Rule 4.4(a) adds into the mix that a lawyer representing a client "shall not . . . use methods of obtaining evidence that violate the legal rights of [a third] person."

Taken together, these three rules (if not Rule 8.4(c) alone) would appear to pose an insurmountable set of ethical obstacles to any attorney personally undertaking an investigation involving deception of any sort. Of course, lawyers are well trained to find ways around problems. So, we might say, since those rules only place shackles upon lawyers (and since we didn't want to do anything that would make us an important fact witness in our client's case anyway), we will simply hire a private detective—Magnum I.P., P.I.—to do the investigation, and let that detective proceed as deceptively as he decides he needs to be.

Published in *Landslide* Volume 4, Number 4, March/April 2012.

As we shift our focus to whether having a third party handle the investigative duties obviates the need to be concerned with the rules in our "how" bucket, a discussion of the first of the rules in our "who" bucket is in order.

Model Rule 5.3 addresses the ethical obligations of lawyers supervising, or having control over, the conduct of others who are not themselves lawyers, but who have been "employed or retained by or associated with" the lawyer. This language is broad enough to apply even to Mr. Magnum. Depending on the lawyer's own roles and responsibilities, Rule 5.3 imposes several levels of more or less stringent ethical requirements flowing from Mr. Magnum's activities. For partners in a law firm, or any other lawyer who "possesses comparable managerial authority," Rule 5.3(a) requires such lawyers to "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that [Mr. Magnum's] conduct is compatible with the professional obligations of the lawyer." As to a lawyer "having direct supervisory authority over" Mr. Magnum, Rule 5.3(b) mandates the lawyer "shall make reasonable efforts to ensure that [Mr. Magnum's] conduct is compatible with the professional obligations of the lawyer." Finally, Rule 5.3(c) imposes direct responsibility for Mr. Magnum's conduct that would be an ethical violation "if engaged in by a lawyer if: (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or (2) the lawyer [is someone who would fit under Rule 5.3(a) or (b)] and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action." The aggregate effect of these requirements should be obvious: Our lawyer still must be concerned with the limitations imposed by Rules 4.1(a), 4.4(a), and 8.4(c), even when she is "merely" involved in the supervision or control of an investigation actually being performed by Mr. Magnum.

There are two other important ethics rules in the "who" bucket about which a lawyer contemplating a pretexting investigation should be aware, and they will likely get lonely if we do not at least make reference to them now. Model Rule 4.2 restricts a lawyer's ability to communicate about a matter with a person known by the lawyer to be represented by another lawyer. The rule requires that if a lawyer wishing to engage in communication with a person "about the subject of the representation" knows that the person is represented by another lawyer "in the matter," then the lawyer may do so only with "the consent of the other lawyer" or when "authorized to do so by law or a court order." Model Rule 4.3 is the yang to Model Rule 4.2's yin. If the person with whom the lawyer wishes to communicate is not represented by counsel, if the lawyer does not know of that representation, or if the communication would not be about the subject of that representation, then the lawyer must adhere to Rule 4.3. That rule prohibits the lawyer "dealing on behalf of a client" from "stat[ing] or imply[ing] that the lawyer is disinterested," and prohibits the lawyer from giving any legal advice ("other than the advice to secure counsel") to the unrepresented person if the lawyer "reasonably should know" that the interests of that person conflict with, "or have a reasonable possibility of" conflicting with, the client's interests. We will now set any further discussion of Rule 4.2 and Rule 4.3 aside for a bit until the subject arises more naturally in our discussion.

If all you knew about the law was the scope of the ethical prohibitions laid out above, then you likely would conclude that lawyers simply cannot condone the use of deceptive tactics in the pursuit of investigations. . . ever. But you know better. Indeed, as observed earlier, certain historical benefits have been achieved through the use of testers in circumstances where lawyers obviously were involved in and aware of the activities. So do those ethical provisions really present any obstacle at all to lawyer involvement in deception when it comes to investigations? The answer is that they certainly do present an obstacle, but how significant of an obstacle is both subject to debate and, as a consequence, far too subjective for intellectual property lawyers to readily draw firm ethical conclusions.

While there is only a smattering of reported cases addressing questions of deceptive behavior by lawyers in connection with intellectual property investigations (and, in fact, there is by no means a wealth of reported cases on the topic outside of the realm of intellectual property), among those courts that have wrestled with the issue, more often than not courts have blessed, or at least not thrown a flag regarding, lawyer involvement in the use of deceptive investigation tactics.

In 1999, the Southern District of New York saw no ethical problem in a lawyer's involvement where an investigator pretended to be a consumer interested in purchasing products and spoke with sales clerks.[3] In *Gidatex, S.r.L. v. Campaniello Imports, Ltd.*, during a lull following years of contentious litigation, Gidatex believed that Campaniello was engaged in a "palming off" scheme in which customers were lured into the store using Gidatex's Saporiti Italia trademark and then sold goods that were deceptively represented to be Saporiti Italia. Gidatex's lawyers tasked investigators with persons pretending to be consumers, interacting with Campaniello sales clerks, and secretly recording the communications.

In justifying what would on its face certainly seem to qualify as "deceptive" conduct, the court explained that the enforcement of trademark laws was an important public policy objective and that pretexting can be effective at uncovering anticompetitive activity that might otherwise go undetected. The court also stressed that such conduct was not unethical because the investigators did not "trick [the sales clerks] into making statements they otherwise would not have made."[4] Rather, the court concluded that all that was captured on tape was Campaniello's normal business practices.

In a much more famous intellectual property dispute, the U.S. District Court for the District of New Jersey similarly concluded that there was nothing wrong with a lawyer's involvement in an investigation that used deception to uncover infringing sales activity in violation of a consent order.[5] In *Apple Corps Ltd. v. International Collectors Society*, the plaintiff previously had obtained a consent order prohibiting the defendant from selling certain stamps bearing the image of John Lennon. Suspecting that the defendant was violating that order, at least one attorney, along with private investigators and others working for the plaintiff's counsel, posed as ordinary consumers and telephoned the defendant's sales representatives to see if the sales representatives would

sell the stamps in question. They did. Thereafter, in response to the defendant's motion for sanctions in light of "deceitful" conduct by the plaintiff's attorneys, the court concluded that Rule 8.4(c) "does not apply to misrepresentations solely as to identity or purpose and solely for evidence-gathering purposes."[6] The court went further in justifying its conclusions: "The prevailing understanding in the legal profession is that a public or private lawyer's use of an undercover investigator to detect ongoing violations of the law is not ethically proscribed, especially where it would be difficult to discover the violations."[7]

More recently, another New York federal court expressly relied upon both *Apple Corps* and *Gidatex* as persuasive authority in concluding that an undercover investigation involving deception was an accepted practice.[8] In *Cartier v. Symbolix, Inc.*, the famous jeweler suspected that an independent jeweler was adding diamonds to the bezels of less expensive Cartier watches and selling them as if they were more expensive Cartier models. Cartier's counsel hired an investigator to purchase one of the "faked" watches. With that proof in hand, Cartier then sought injunctive relief to stop the sales. The independent jeweler, Symbolix, sought to defend against Cartier's request for an injunction on the basis of Cartier's "unclean hands" in the undercover investigation, but the court echoed the sentiment expressed in *Gidatex* and *Apple Corps* that the "prevailing understanding in the legal profession" is that using an "undercover investigator to detect ongoing violations of the law is not ethically proscribed, especially where it would be difficult to discover the violation by other means."[9]

In addition to cases like *Gidatex*, *Apple Corps*, and *Cartier* where courts expressly addressed such questions, a number of others reflect quite clearly that lawyers were involved with, or aware of, investigators who were acting under pretext in furtherance of obtaining evidence to prove intellectual property violations, but the courts simply said nothing about the issue at all.[10]

There is, however, at least one court that has not looked as favorably on lawyer involvement in pretextual investigations.[11] In *Midwest Motor Sports v. Arctic Cat Sales, Inc.*,[12] the only federal appellate court decision directly addressing this subject, the Eighth Circuit indicated clearly that it was bothered by the role of attorneys in a deceptive investigation which, in many respects, was quite similar to Gidatex's. One of Arctic Cat's former franchise dealers sued on a theory that Arctic Cat had wrongfully terminated its franchise. Arctic Cat's lawyer retained a former FBI agent to visit the former dealer's place of business. The former FBI agent, Mohr, posed as an interested snowmobile buyer in order to gather evidence helpful to defending the lawsuit against Arctic Cat, focusing on things like what products were being promoted in the showroom and what brands were selling best, and secretly recording his conversations about those topics. The court concluded that Arctic Cat's attorneys should be sanctioned for their involvement in the secret recording and that the audiotapes of those conversations should be excluded from evidence.

While that story (other than the outcome) should sound very familiar, there is an important difference in the facts in *Midwest Motor Sports*. Unlike the investigators in *Gidatex*, Mohr spoke not just with low-level sales employees but also with certain management-level employees. Such conduct implicates the two ethics rules in our "who" bucket that we earlier looked at only briefly: Rules 4.2 and 4.3. The communications with management-level employees matters to any Rule 4.2 analysis because under both the Model Rules and many state variations of it, management-level employees often are treated as being represented by the lawyer representing the organization. The court believed that the lawyer's involvement was unethical because Mohr's communications with certain employees was the type that would have violated Rule 4.2 if Mohr had been a lawyer. However, the outcome in *Arctic Cat* cannot be distinguished solely on that basis, as the Eighth Circuit also concluded that the lawyer's conduct ran afoul of Rule 8.4(c) because the duty imposed by that rule "to refrain from conduct that involves deceit or misrepresentation should preclude any attorney from participating in the type of surreptitious conduct that occurred here" and that "[s]uch tactics fall squarely within Model Rule 8.4(c)'s prohibition."[13]

While the case law may indicate that intellectual property lawyers have a good chance of convincing a court that a deceptive investigation was appropriate, disciplinary authorities may also take an interest, and at first blush, reconciling the use of deception in investigations with the language of the ethics rules themselves seems difficult. Nevertheless, at least two ethics opinions, despite finding no support for such a position in the text of the rules, have treated some deceptive investigative activities as ethical.

In 2007, the Alabama State Bar Office of General Counsel opined that "[d]uring pre-litigation investigation of suspected infringers of intellectual property rights, a lawyer may employ private investigators to pose as customers under the pretext of seeking services of the suspected infringers on the same basis or in the same manner as a member of the general public."[14] The portions of the Alabama opinion that are not obviously result oriented amount to a model of poor analysis. The opinion's treatment of Rule 8.4(c) was straightforward in its result-oriented approach—declaring that Rule 8.4(c) is not intended to apply to misrepresentations as to identity and purpose when the misrepresentations are used "to detect ongoing violations of the law where it would be difficult to discover those violations by any other means."[15] Beyond that aspect, the opinion ignores altogether the applicability of Rule 4.1, and attempts to brush aside Rule 4.2 and Rule 4.3 concerns by concluding, respectively, that one cannot be a "party" until a lawsuit has actually been filed, and that a lawyer acting as an investigator is not "acting in his capacity as a lawyer—'dealing on behalf of a client.'"[16] Both of those conclusions are, in a word, bizarre.[17]

Another ethics opinion issued in 2007 by another entity—the New York County Lawyers Association Committee on Professional Ethics—suffers not from the type of analytical flaws that pervade the Alabama opinion, but merely from

Brian S. Faughnan practices law in Memphis with Thomason Hendrix Harvey Johnson & Mitchell, PLLC. In addition to representing lawyers and law firms, He focuses his practice on appellate law and commercial litigation. He can be reached at faughnanb@thomasonlaw.com.

the kind of general unhelpfulness that comes from any set of overly-stipulated conduct guidelines.[18] The New York County opinion concluded that it was "generally unethical for a non-government lawyer to knowingly utilize and/or supervise an investigator who will employ dissemblance in an investigation," but provided a limited exception permitting such conduct "in a small number of exceptional circumstances where the dissemblance by investigators is limited to identity and purpose and involves otherwise lawful activity undertaken solely for the purpose of gathering evidence."[19] That opinion specifically delineated the exceptional circumstances as when (1) the dissemblance is expressly authorized by law or the subject matter of the investigation is a violation of intellectual property rights or civil rights that the lawyer believes in good faith is or imminently will be occurring, and (2) the evidence sought by the investigation is not reasonably available through lawful means. Unfortunately, the committee did not stop there, but went on to muddy the waters by adding that "the lawyer's conduct and the investigator's conduct [must] not otherwise violate the [New York attorney ethics rules] or applicable law" and that "the dissemblance [must] not unlawfully or unethically violate the rights of third parties."[20]

Other, more recent, ethics opinions focusing on a specific type of pretexting activity—the making of a "friend" request on a social media platform for the purpose of gathering information that the user would otherwise only share with certain persons—raise further questions for intellectual property lawyers regarding the ethical propriety of deceptive conduct.

In 2009, the Professional Guidance Committee of the Philadelphia Bar Association opined that it would be a violation of Rule 8.4(c) for a lawyer to have a third party send a MySpace friend request to a witness without affirmatively disclosing to the recipient that the purpose for the friend request was to obtain and share information with the lawyer that could be used to impeach the witness's prior deposition testimony.[21] Just one year later, in 2010, the New York City Bar Association's Committee on Professional and Judicial Ethics offered similar guidance nixing the idea that a lawyer could personally, or through an agent, create a pseudonymous profile on Facebook for the purpose of attempting to "friend" an unrepresented adversary and, thereby, gain access to information that would otherwise be shielded from view.[22] As with the Philadelphia Bar, the New York City Bar opinion cited Rule 8.4's prohibition on deceptive or misleading conduct, but also explicitly referenced Rules 4.1 and 5.3(b).

Whether you find those two conclusions to be a bit Pollyanna-ish and troubling, or you find it troubling that other bodies charged with issuing ethics opinions appear to simply ignore the plain text of the rules governing their analysis to permit deceptive investigative activity, all lawyers should agree that the existence of a rule as overreaching as Rule 8.4(c) plays a large role in creating such troubling outcomes. After all, what sense does it even make to have a rule that we know for certain cannot be extended to its full, literal extent?

For example, assume you see me in the elevator and ask, "How are you?" I know that you likely really only want me to respond consistently with social convention and say, "I'm fine," even if the only honest answer would be for me to say, "I've had a horrible morning and am generally feeling just awful." But no one should ever seriously contend that by responding with "I'm fine," I have committed an ethics violation even though the text of Model Rule 8.4(c) flatly prohibits dishonesty by lawyers and does not tie its prohibition to the representation of a client. Or, if my first example seems unnecessarily convoluted, then think of a lawyer who is also a successful professional poker player or, even closer to home, think of how you have answered questions in the past from children, whether yours or not, regarding the existence of certain holiday gift givers.

The usual answer to such criticism regarding Rule 8.4(c)'s breadth is that, according to the Scope section of the Model Rules, "The Rules of Professional Conduct are rules of reason. They should be interpreted with reference to the purposes of legal representation and of the law itself."[23] Yet, wouldn't it be better to fix the problem more directly? Some states have officially embraced the reality that lawyers can and actually do have involvement with surreptitious investigations that involve deceptive conduct, and have offered a more direct fix by adopting variations in the black letter of their versions of Rule 8.4, or through adoption of comments to that rule, that specifically exempt involvement in legitimate investigative activities from the prohibition on "dishonesty, fraud, deceit or misrepresentation."[24]

Among those approaches, Virginia's is perhaps the most intriguing. Virginia adopted a version of Rule 8.4(c) that adds the modifying clause, "which reflects adversely on the lawyer's fitness to practice law," to limit what types of dishonesty, fraud, deceit, or misrepresentation constitute an ethics violation.[25] Such a rule would appear to have the benefit of allowing lawyers engaged in investigations of intellectual property matters that involve some deceptive conduct to rest a bit easier in terms of being able to justify their conduct and reduce their potential disciplinary exposure, at least as long as it is agreed that dishonesty, deceit, or misrepresentations in that context would not reflect adversely on the lawyer's fitness to practice law. Such a rule better reconciles the plain (and presently extremely expansive) language of such a rule with the reality that a wide variety of conduct, whether it be bluffing in poker, telling children that a magical being descends down the chimney to bring them presents ("Yes, Virginia. Your Rule 8.4(c) specifically lets lawyers say there is a Santa Claus!"), or misrepresenting how you are feeling in an elevator, is dishonest in a technical, definitional sense but ought never be the fodder for a disciplinary complaint.

Of course, any rules-based fix that would focus only on Rule 8.4(c) would not go far enough. Squaring the practical reality of surreptitious investigations with the ethics rules involves a larger fix in the nature of a rule that would say something like: "Notwithstanding Rules 4.1(a), 4.3, 4.4(a), and [8.4], it shall not be professional misconduct for a lawyer in the course of representing a client to advise the client or others about, or to supervise personally or through others, lawful covert activity in the investigation of illegal or unlawful activities, provided that the lawyer's conduct otherwise complies with these rules."[26] Adoption of such a specific rules-based exception allowing lawyer involvement in surreptitious investigation activities offers advantages to both lawyers and to the integrity of the

ethics rules themselves. For lawyers, such a rule would allow for much greater certainty in evaluating potential conduct. As to the integrity of the rules themselves, the rule would treat this issue in a much more straightforward and realistic manner rather than leaving it to courts and others to attempt to fashion public policy-based exceptions to justify certain approaches considered to be acceptable law practice, plain language of the ethics rules notwithstanding.

In the meantime, for lawyers looking for some practical guidance over and above the obvious need to be familiar with the rules, ethics opinions, and case law of note in the jurisdiction in which you are licensed and (if different) of the jurisdiction where a contemplated investigation will occur, the above authorities can be synthesized in a relatively straightforward fashion: If your investigators go beyond employing deception simply as to who they are and why they are asking, and employ deception to cause someone to do or say something they otherwise ordinarily would not have said, then a lawyer can expect that a court or disciplinary counsel will be significantly more likely to find the lawyer's involvement to be problematic. ■

Endnotes

1. 18 U.S.C. § 1039 (2006).

2. *See, e.g.*, Hill v. Shell Oil Co., 209 F. Supp. 2d 876 (N.D. Ill. 2002).

3. Gidatex, S.r.L. v. Campaniello Imps., Ltd., 82 F. Supp. 2d 119 (S.D.N.Y. 1999).

4. *Id.* at 126.

5. Apple Corps Ltd. v. Int'l Collectors Soc'y, 15 F. Supp. 2d 456 (D.N.J. 1998).

6. *Id.* at 475.

7. *Id.*

8. Cartier v. Symbolix, Inc., 386 F. Supp. 2d 354 (S.D.N.Y. 2005).

9. *Id.* at 362.

10. *See, e.g.*, Louis Vuitton S.A. v. Spencer Handbags Corp., 765 F.2d 966 (2d Cir. 1985); Phillip Morris USA Inc. v. Shalabi, 352 F. Supp. 2d 1067 (C.D. Cal. 2004); A.V. by Versace, Inc. v. Gianni Versace, S.p.A., Nos. 96 CIV. 9721PKLTHK, 98 CIV. 0123PKLTHK, 2002 WL 2012618 (S.D.N.Y. Sept. 3, 2002); Nikon, Inc. v. Ikon Corp., 803 F. Supp. 910 (S.D.N.Y. 1992), *aff'd* 987 F.2d 91 (2d Cir. 1993).

11. There are a number of cases outside of the intellectual property arena that should cause lawyers to be very cautious about assuming that they can safely be involved in deceptive conduct even if they believe the ends justify such means. *See, e.g.*, Allen v. Int'l Truck & Engine, No. 1:02-cv-0902-RLY-TAB, 2006 U.S. Dist. LEXIS 63720 (S.D. Ind. Sept. 6, 2006) ("[L]awyers (and investigators) cannot trick protected employees into doing things or saying things they otherwise would not say or do"); *In re* Pautler, 47 P.3d 1175 (Colo. 2002) (involving prosecutor who impersonated a public defender to secure a murder suspect's surrender); *In re* Ositis, 40 P.3d 500 (Or. 2002) (imposing reprimand on attorney who employed investigator to pose as journalist to glean information from adversary); *In re* Gatti, 8 P.3d 966 (Or. 2000) (rejecting exceptions to permit deception prohibited by the ethics rules even for governmental lawyers or civil rights investigators); *but see In re* Hurley, No. 2007AP478-D (Wis. Feb. 11, 2009) (declining to discipline lawyer involved in deceptive conduct aimed at obtaining exculpatory evidence for a defendant facing child pornography charges).

12. 347 F.3d 693 (8th Cir. 2003).

13. *Id.* at 699–700.

14. Ala. State Bar Office of Gen. Counsel, Formal Op. 2007-05, at 1.

15. *Id.* at 5.

16. *Id.* at 4.

17. Federal courts, for example, have had no difficulty concluding that Model Rule 4.2 applies to communications occurring before a lawsuit was filed. *See, e.g.*, Penda Corp. v. STK, LLC, Nos. Civ.A. 03-5578, Civ.A. 03-6240, 2004 WL 1628907 (E.D. Pa. July 16, 2004) (citing United States v. Grass, 239 F. Supp. 2d 535, 540–41 (M.D. Pa. 2003)).

18. N.Y. Cnty. Lawyers Ass'n Comm. on Prof'l Ethics, Formal Op. 737 (2007).

19. *Id.* at 1.

20. *Id.*

21. Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02.

22. N.Y. City Bar Ass'n Comm. on Prof'l & Judicial Ethics, Formal Op. 2010-2.

23. Model Rules of Professional Conduct Scope [14] (2010).

24. *See* Fla. Rules of Prof'l Conduct R. 8.4(c); Iowa Rules of Prof'l Conduct R. 8.4 cmt. [6]; Ohio Rules of Prof'l Conduct R. 8.4 cmt. [2A]; Or. Rules of Prof'l Conduct R. 8.4(b); Va. Rules of Prof'l Conduct R. 8.4(c).

25. Va. Rules of Prof'l Conduct R. 8.4(c).

26. Douglas R. Richmond, Brian S. Faughnan & Michael L. Matula, Professional Responsibility in Litigation 207 (2011).

ETHICAL IMPLICATIONS OF LAWYER PRETEXTING

Kathryn M. Fenton*
Jones Day

I. Introduction

A. Recent headlines have highlighted a number of instances in which lawyers (or others working at their direction such as legal assistants or private investigators) have been accused of unlawful "pretexting." *See, e.g.*, Kevin Paulsen, *First 'Pretexting' Charges Filed Under Law Passed After HP Spy Scandal*, WIRED.COM (Jan. 9, 2009), *available at* http://www.wired.com/threatlevel/2009/01/first-pretextin/; Joan C. Rogers, *Scandals Involving Investigators Ensnare Lawyers*, 22 LAW. MAN. PROF. CONDUCT 501 (2006). Social media sites such as Facebook also raise this issue when lawyers misrepresent their identity or purpose in visiting the site. Steven C. Bennett, *Ethics of Lawyer Social Networking*, 73 ALBANY L. REV. 113 (2009); Tom Mighell, *Avoiding a Grievance in 140 Characters or Less: Ethical Issues in Social Media and Online Activities*, 51 ADVOC. (TEXAS) 8 (2010).

B. Ethical rules have recognized that pretexting or "dissemblance" occurs when a lawyer engages in fraud or deceit or obtains information or evidence for use in litigation or internal investigations through false pretenses or deception. Pretexting by lawyers can take a variety of forms, including:

1. Misrepresenting one's true identity to telephone service providers in order to obtain telephone records for use in internal investigations;

2. Posing as a customer and seeking to purchase goods to support infringement claim; or

3. Instructing investigator to "friend" adverse witness on Facebook to see impeachment evidence.

C. Additional questions about lawyer pretexting may arise during pre-trial and trial proceedings.

1. Can lawyer use social media as tool to assist in jury selection?

2. Can lawyer monitor Internet postings by jurors during trial, seeking evidence of juror misconduct?

3. If lawyer discovers such postings, can lawyer use information on behalf of client or is there obligation to report juror misconduct to court?

---

* The opinions expressed herein are those of Ms. Fenton alone and not necessarily those of Jones Day or its clients.

D. In thinking about such activities, it is important for lawyers to understand the larger set of ethical issues presented by pretexting. These issues include:

1. Under what circumstances, if any, are lawyers ethically permitted to engage in pretexting/dissemblance?

2. Under what circumstances is it ethically permissible for lawyers to supervise investigator who engages in pretexting?

3. Do such activities always constitute fraud, deceit or misrepresentation in violation of the rules of professional responsibility?

4. Are ethics rules different for government lawyers who may need to supervise pretexting as part of law enforcement activities?

E. This outline reviews the guidance currently available on lawyer pretexting and identifies associated open issues that require further clarification by courts and ethics bodies.

II. Relevance to Antitrust and Consumer Protection Attorneys

A. Many in-house and outside counsel employed by corporate law firms have given relatively little thought to the ethical issues of pretexting, thinking such practices involve "cloak and dagger" activities far removed from their day-to-day clients. Yet, as recent headlines have demonstrated, there are numerous circumstances in which such activities may arise in a corporate context, including:

1. Investigating alleged employment discrimination;

2. Wiretapping to investigate possible breach of contract;

3. Acquiring evidence of potentially infringing products;

4. Setting up fake web site as part of consumer protection "sting";

5. Seeking impeachment evidence to discredit trial witnesses;

6. Monitoring social media for jury selection; and

7. Monitoring post-trial use by juror of social media to obtain evidence to support new trial application.

B. Indeed, all lawyers may need to consider potentially resorting to such activities as part of their obligation under ABA Model Rule 1.1 to provide zealous and competent representation of their clients. Some commentators have suggested that there may be situations in which zealous representation of a client's interest may require resorting to some form of deception. Monroe H. Freedman, *The Praise of Overzealous Representation—Lying to Judges, Deceiving Third Parties,*

III. Ethical Rules Implicated by Pretexting

A. Courts and ethics opinions have found that numerous ethical rules can be implicated by pretexting activities. For example,

1. ABA Model Rule 4.1(a): In the course of representing a client, "a lawyer shall not knowingly. . . make a false statement of material fact or law to a third party."

2. ABA Model Rule 4.2: Lawyer shall not communicate "about the subject matter of a representation with a person who the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order."

3. ABA Model Rule 8.4(c): It is "professional misconduct" for a lawyer "to engage in conduct involving dishonesty, fraud, deceit, or misrepresentation."

4. ABA Model Code DR 7-102(A)(5): "A lawyer shall not misrepresent his or her identity while engaged in the practice of law."

B. There are additional ethical considerations that are presented when the pretexting arises during pre-trial and trial proceedings.

1. ABA Model Rule 3.5, Impartiality And Decorum Of The Tribunal, provides that lawyer shall not:

(a) Seek to influence a judge, juror, prospective juror or other official by means prohibited by law;

(b) Communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order;

(c) Communicate with a juror or prospective juror after discharge of the jury if

(i) The communication is prohibited by law or court order

(ii) The juror has made known to the lawyer a desire not to communicate; or

(iii) The communication involves misrepresentation, coercion, duress or harassment; or

(d) Engage in conduct intended to disrupt a tribunal.

C. These rules apply whether the pretexting activities were undertaken directly by lawyer or by another (such as legal assistant or investigator) acting at lawyer's direction. The Rules of Professional Responsibility make clear that using the services of a third party cannot be a means of circumventing the lawyer's personal ethical obligations. *See, e.g.*,

1. ABA Model Rule 5.3: Lawyer is responsible for another person's violation through involvement, knowledge, or supervisory authority if lawyer orders, directs, or ratifies the conduct.

2. ABA Model Rule 8.4(a): Lawyer cannot circumvent ethical prohibitions "through acts of another."

IV. Judicial Decisions and Ethics Opinions Dealing with Pretexting

A. Notwithstanding the relatively short period of time that such issues have been considered, there already are a number of court decisions and ethics opinions that have addressed pretexting issues.

B. Court Decisions

1. *In re Crossan*, 880 N.E. 2d 352 (Mass. 2008) (disbarring two attorneys who conducted false employment interviews with judge's former law clerk in attempt to gain evidence of judicial bias).

2. *In re Paulter*, 47 P.3d 1175 (Colo. 2002) (upholding discipline against deputy district attorney who misrepresented his identity to criminal suspect).

3. *In re Ositis*, 40 P.3d 500 (Or. 2002) (whether or not lawyer actually directed private investigator to pose as journalist and interview party to potential legal dispute, lawyer played major role in scheme and thus bore responsibility for it directly as well as vicariously).

4. *In re Gatti*, 8 P.3d 966 (Or. 2000) (upholding discipline against lawyer who misrepresented his identity to insurance company).

5. *Allen v. International Truck and Engine*, 2006 U.S. Dist. LEXIS 63720 (S.D. Ind. 2006) (attorneys violated Model Rules by directing investigators to pose as employees and question employees about litigation with the company).

6. *Midwest Motor Sports v. Arctic Cat Sales, Inc.*, 347 F.3d 693 (8th Cir. 2003) (unethical for defense counsel to instruct investigator to pose as plaintiff's customer in order to elicit admissions regarding litigation).

7. *Gidatex S.r.L. v. Companiello Imports Ltd.*, 82 F. Supp. 2d 119 (S.D.N.Y. 1999) (lawyer for furniture manufacturer did not violate ex parte contact rule by sending undercover investigators posing as consumers to talk with former distributor's employees to verify whether distributor was infringing on manufacturer's trademark).

8. *Apple Corps Ltd. v. International Collectors Society*, 15 F. Supp. 2d 456 (D.N.J. 1998) (to investigate possible IP infringement, lawyer could pose as customer of alleged infringer).

9. *In re Wood*, 526 N.W.2d 513 (Wis. 1995) (lawyer suing former client violated Rule 8.4(c) by hiring private investigator to obtain copy of client's insurance policy, knowing that only way investigator could do so was by misrepresenting himself to insurance company).

C. Ethics Opinions

1. San Diego County Bar Legal Ethics Op. 2011-2 (May 24, 2011), which found that a lawyer may not send "friend" request to opponent or potential witness with goal of getting inside information for client's matter.

   (a) The opinion considered a hypothetical in which plaintiff's counsel in wrongful discharge actions sent "friends" request to two high-ranking company employees whom his client had identified as being dissatisfied with their employer.

   (b) As "high-ranking employees," it was likely that individuals in question were part of represented corporate party for purposes of Cal. Rule of Prof. Conduct 2-100, which prohibits lawyers from communicating with represented party without consent of party's lawyer. Thus, the social media contact represented an:

      (i) Indirect ex parte communication, and

      (ii) The motivation for "friends" request clearly established its connection to subject matter of representation.

   (c) The opinion also found that "the attorney's duty not to deceive prohibits him from making a friend request even of unrepresented witnesses without disclosing the purpose of the request."

2. New York County Ass'n Comm. on Professional Ethics Op. 737 (May 23, 2007) held that "dissemblance" by lawyers could be permitted under

(a) Either (i) the purpose of the investigation is to probe a violation of civil rights or intellectual property rights and the lawyer believes in good faith that the violation is taking place or is imminent, or (ii) the dissemblance is expressly authorized by law;

(b) The evidence sought is not reasonably and readily available through other lawful means;

(c) The conduct of the lawyer and the investigator does not otherwise violate the New York Code of Professional Responsibility or applicable law; and

(d) The dissemblance does not unlawfully or unethically violate the rights of third persons.

(e) In addition, Op. 737 cautioned:

(i) The investigator must be instructed not to elicit information protected by attorney-client privilege; and

(ii) "In most cases, the ethical bounds of permissible conduct will be limited to situations involving the virtual necessity of non-attorney investigator(s) posing as an ordinary consumer(s) engaged in an otherwise lawful transaction in order to obtain basic information not otherwise available."

3. NYCBA Formal Op. 2010-2 found that lawyer may not attempt to gain access to social networking website under false pretenses, either directly or through agent.

4. NY State Bar Ass'n Opin. 843 (Sept. 10, 2010) approved use of public website information and concluded Rule 8.4 was not implicated because lawyer is not engaging in deception by accessing public portions of network. According to the opinion, this is no different than relying on print media or paid research services.

5. Ala. Op. 2007-05 found that during investigation of possible IP infringement a lawyer may pose as customer under the pretext of seeking services of suspected infringers on the same basis or in the same manner as a member of the general public.

6. Penn. Op. 2009-02 (March 2009) concluded that a lawyer would violate ethical rules by employing investigator to "friend" an adverse witness on Facebook for the collection of impeachment evidence.

7. The ABA expressly has declined to address issue. *See* ABA Formal Op. 01-422 (June 2001).

V. Do the Same Rules Apply to Government Attorneys?

A. There has been significant and ongoing debate as to whether the ethical prohibitions on pretexting should apply with the same force to government attorneys who must engage in or supervise such activities as part of their law enforcement roles.

1. One line of argument emphasizes the importance of ensuring that legitimate law enforcement efforts are not impeded by an unduly restrictive set of ethical concerns and concludes that government attorneys have a greater scope in this regard because of their investigative roles.

2. The opposing school of thought emphasizes that, as public-servants, government attorneys should be held to the highest ethical standards and serve as a model for the rest of the bar. Thus, despite the law enforcement justification, proponents of this approach would apply the same ethical standards to government attorneys.

B. Only a handful of jurisdictions have addressed this question in their ethical rules. The majority expressly permit covert action by government attorneys as part of law enforcement role.

1. *See, e.g.*, Oregon Rule 8.4(b) ("[I]t shall not be professional misconduct for a lawyer to advise clients or others about or to supervise lawful covert activity in the investigation of violations of civil or criminal law or constitutional rights, provided the lawyer's conduct is otherwise in compliance with these Rules of Professional Conduct. 'Covert activity,' as used in this rule, means an effort to obtain information on unlawful activity through the use of misrepresentations or other subterfuge. 'Covert activity' may be commenced by a lawyer or involve a lawyer as an advisor or supervisor only when the lawyer in good faith believes there is a reasonable possibility that unlawful activity has taken place, is taking place or will take place in the foreseeable future.");

2. Florida Rule 4-8.4(e) ("A lawyer shall not . . . engage in conduct involving dishonesty, fraud, deceit, or misrepresentation, except that it shall not be professional misconduct for a lawyer for a criminal law enforcement agency or regulatory agency to advise others about or to supervise another in an undercover investigation, unless prohibited by law or rule, and it shall not be professional misconduct for a lawyer employed in a capacity other than as a lawyer by a criminal law enforcement agency or regulatory agency to participate in an undercover investigation; unless prohibited by law or rule . . . .").

C. Other jurisdictions have issued ethics opinions that address pretexting by government lawyers. *See, e.g.,*

1. D.C. Op. 323 (2004) (lawyers employed by government agencies who act in a non-representational official capacity in manner they reasonably believe to be authorized by law do not violate Rule 8.4 if, in the course of their employment, they make misrepresentations that are reasonably intended to further the conduct of their official duties);

2. Utah Ethics Op. 02-05 (2002) (government attorney's "lawful participation in a lawful government operation" does not violate Rule 8.4 if deceit is "required in the successful furtherance" of undercover activity);

3. Va. Legal Ethics Op. 1765 (2003) ("When an attorney employed by the federal government uses lawful methods such as the use of 'alias identities' and non-consensual tape-recording, as part of his intelligence or covert activities, those methods cannot be seen as reflecting adversely on his fitness to practice law; therefore such conduct will not violate the prohibition in Rule 8.4(c).").

VI. How to Resolve Questions Regarding the Appropriateness of Pretexting

A. Only a handful of jurisdictions have attempted to address pretexting by a specific rule and, even in these cases, the rule often addresses only a limited category of activity. *See, e.g.*, Oregon Rule 8.4(b) ("It shall not be professional misconduct for a lawyer to advice clients or others about or to supervise lawful convert activity *in the investigation of violations of civil or criminal law or constitutional rights. . . .*") (emphasis added).

B. In those jurisdictions that do not address undercover investigations and similar activities in their ethics rules, lawyers must rely on public policy arguments embodies in cases refusing to find attorney misconduct in participating in "sting" investigations. *See, e.g.,*

1. *Apple Corps. Ltd. v. International Collectors Soc'y*, 15 Supp. 2d 456 (D.N.J. 1998);

2. *Gidatex S.r.L. v. Companiello Imports Ltd.*, 82 F. Supp. 2d 119 (S.D.N.Y. 1999);

3. *But see Sequa Corp. v. Lititech Inc.*, 807 F. Supp. 653 (D. Col. 1992) (lawyers in private practice may not use deception to investigate disciplinary violations).

VII. Potential Consequences of Pretexting Violations

A. In addition to possible disciplinary proceedings against the individual lawyer, there are other potential penalties and sanctions resulting from pretexting by lawyers.

B. Depending on the circumstances, penalties and sanctions may include:

1. Criminal and civil liability under

(a) Gramm-Leach-Bliley Act;

(b) Mail / wire fraud statutes;

(c) FTC Act;

(d) State statutes.

2. Waiver of attorney-client privilege (due to crime/fraud exception)

3. Exclusion of evidence in litigation

VIII. Other Considerations Before Using Pretexting in Corporate Investigations

A. Determine whether you are in a jurisdiction where pretexting or similar activities by a lawyer already have been reviewed by local authorities and approved or tolerated. Otherwise, you are potentially breaking new ground and hearing all the risks that entails.

B. In addition to ethics rules, review other statutes possibly affecting legal status of pretexting.

C. Ensure your client is prepared for potential press coverage and public relations fallout if pretexting activities become public.

D. To be safe, pretexting should only be used to obtain objective information available to the general public

IX. Additional Resources

A. Steven C. Bennett, *Ethics of "Pretexting" in a Cyber World*, 41 MCGEORGE L. REV. 271 (2010).

B. Barry R. Temkin, *Deception in Undercover Investigations: Conduct-Based v. Status-Based Ethical Analysis*, 32 SEATTLE U.L. REV. 123 (2008).

C. William H. Fortune, *Lawyers, Covert Activity, and Choice of Evils*, 32 J. LEGAL PROF. 99 (2008).

D. Kevin Bank, *Not Telling the Whole Truth: How Much Leeway Do Lawyers or Investigators Working with Them Have to Feign Identity?*, WASH. STATE BAR NEWS, June 2008, *available at* http://www.wsba.org/media/publications/barnews/jun08-bank.htm.

E. Gerald B. Lefcourt, *Fighting Fire with Tire: Private Attorneys Using the Same Investigative Techniques as Government Attorneys: The Ethical and Legal Considerations for Attorneys Conducting Investigations*, 36 HOFSTIA L. REV. 397 (2007).

F. Ray V. Hartwell, III, *Compliance and Ethics in Investigations: Getting it Right*, THE ANTITRUST SOURCE (Dec. 2006), *available at* http://www.abanet.org/antitrust/at-source/06/12/Dec06-Hartwell12=19f.pdf.

G. Robert L. Reibold, *Hidden Dangers of Using Private Investigators*, 17 S.C. LAW 18 (July 2005).

H. David B. Isbell and Lucantonia N. Salvi, *Ethical Responsibilities of Lawyers for Deception by Undercover Investigators and Discrimination Testers: An Analysis of the Provision Prohibiting Misrepresentation Under the Model Rules of Professional Conduct*, 8 GEO. J. LEGAL ETHICS 791 (1995).

NEW YORK STATE UNIFIED COURT SYSTEM

PART 1200

RULES OF PROFESSIONAL CONDUCT

Dated: January 1, 2017

These Rules of Professional Conduct were promulgated as Joint Rules of the Appellate Divisions of the Supreme Court, effective April 1, 2009, and amended on several occasions thereafter. They supersede the former part 1200 (Disciplinary Rules of the Code of Professional Responsibility).

The New York State Bar Association has issued a Preamble, Scope and Comments to accompany these Rules. They are not enacted with this Part, and where a conflict exists between a Rule and the Preamble, Scope or a Comment, the Rule controls.

This unofficial compilation of the Rules provided for informational purposes only. The official version of Part 1200 is published by the New York State Department of State. An unofficial on-line version is available at www.dos.ny.gov/info/nycrr.html (Title 22 [Judiciary]; Subtitle B Courts; Chapter IV Supreme Court; Subchapter E All Departments; Part 1200 Rules of Professional Conduct; § 1200.0 Rules of Professional Conduct).

TABLE OF CONTENTS

Page

Page

Page

PART 1200 - RULES OF PROFESSIONAL CONDUCT

RULE 1.0.

Terminology

(a) "Advertisement" means any public or private communication made by or on behalf of a lawyer or law firm about that lawyer or law firm's services, the primary purpose of which is for the retention of the lawyer or law firm. It does not include communications to existing clients or other lawyers.

(b) "Belief" or "believes" denotes that the person involved actually believes the fact in question to be true. A person's belief may be inferred from circumstances.

(c) "Computer-accessed communication" means any communication made by or on behalf of a lawyer or law firm that is disseminated through the use of a computer or related electronic device, including, but not limited to, web sites, weblogs, search engines, electronic mail, banner advertisements, pop-up and pop-under advertisements, chat rooms, list servers, instant messaging, or other internet presences, and any attachments or links related thereto.

(d) "Confidential information" is defined in Rule 1.6.

(e) "Confirmed in writing" denotes (i) a writing from the person to the lawyer confirming that the person has given consent, (ii) a writing that the lawyer promptly transmits to the person confirming the person's oral consent, or (iii) a statement by the person made on the record of any proceeding before a tribunal. If it is not feasible to obtain or transmit the writing at the time the person gives oral consent, then the lawyer must obtain or transmit it within a reasonable time thereafter.

(f) "Differing interests" include every interest that will adversely affect either the judgment or the loyalty of a lawyer to a client, whether it be a conflicting, inconsistent, diverse, or other interest.

(g) "Domestic relations matter" denotes representation of a client in a claim, action or proceeding, or preliminary to the filing of a claim, action or proceeding, in either Supreme Court or Family Court, or in any court of appellate jurisdiction, for divorce, separation, annulment, custody, visitation, maintenance, child support or alimony, or to enforce or modify a judgment or order in connection with any such claim, action or proceeding.

(h) "Firm" or "law firm" includes, but is not limited to, a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other

association authorized to practice law; or lawyers employed in a qualified legal assistance organization, a government law office, or the legal department of a corporation or other organization.

(l) "Fraud" or "fraudulent" denotes conduct that is fraudulent under the substantive or procedural law of the applicable jurisdiction or has a purpose to deceive, provided that it does not include conduct that, although characterized as fraudulent by statute or administrative rule, lacks an element of scienter, deceit, intent to mislead, or knowing failure to correct misrepresentations that can be reasonably expected to induce detrimental reliance by another.

(j) "Informed consent" denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated information adequate for the person to make an informed decision, and after the lawyer has adequately explained to the person the material risks of the proposed course of conduct and reasonably available alternatives.

(k) "Knowingly," "known," "know," or "knows" denotes actual knowledge of the fact in question. A person's knowledge may be inferred from circumstances.

(l) "Matter" includes any litigation, judicial or administrative proceeding, case, claim, application, request for a ruling or other determination, contract, controversy, investigation, charge, accusation, arrest, negotiation, arbitration, mediation or any other representation involving a specific party or parties.

(m) "Partner" denotes a member of a partnership, a shareholder in a law firm organized as a professional legal corporation or a member of an association authorized to practice law.

(n) "Person" includes an individual, a corporation, an association, a trust, a partnership, and any other organization or entity.

(o) "Professional legal corporation" means a corporation, or an association treated as a corporation, authorized by law to practice law for profit.

(p) "Qualified legal assistance organization" means an office or organization of one of the four types listed in Rule 7.2(b)(1)-(4) that meets all of the requirements thereof.

(q) "Reasonable" or "reasonably," when used in relation to conduct by a lawyer, denotes the conduct of a reasonably prudent and competent lawyer. When used in the context of conflict of interest determinations, "reasonable lawyer" denotes a lawyer acting from the perspective of a reasonably prudent and

competent lawyer who is personally disinterested in commencing or continuing the representation.

(r) "Reasonable belief" or "reasonably believes," when used in reference to a lawyer, denotes that the lawyer believes the matter in question and that the circumstances are such that the belief is reasonable.

(s) "Reasonably should know," when used in reference to a lawyer, denotes that a lawyer of reasonable prudence and competence would ascertain the matter in question.

(t) "Screened" or "screening" denotes the isolation of a lawyer from any participation in a matter through the timely imposition of procedures within a firm that are reasonably adequate under the circumstances to protect information that the isolated lawyer or the firm is obligated to protect under these Rules or other law.

(u) "Sexual relations" denotes sexual intercourse or the touching of an intimate part of the lawyer or another person for the purpose of sexual arousal, sexual gratification or sexual abuse.

(v) "State" includes the District of Columbia, Puerto Rico, and other federal territories and possessions.

(w) "Tribunal" denotes a court, an arbitrator in an arbitration proceeding or a legislative body, administrative agency or other body acting in an adjudicative capacity. A legislative body, administrative agency or other body acts in an adjudicative capacity when a neutral official, after the presentation of evidence or legal argument by a party or parties, will render a legal judgment directly affecting a party's interests in a particular matter.

(x) "Writing" or "written" denotes a tangible or electronic record of a communication or representation, including handwriting, typewriting, printing, photocopying, photography, audio or video recording, e-mail or other electronic communication or any other form of recorded communication or recorded representation. A "signed" writing includes an electric sound, symbol or process attached to or logically associated with a writing and executed or adopted by a person with the intent to sign the writing.

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.

(b) A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it.

(c) lawyer shall not intentionally:

(1) fail to seek the objectives of the client through reasonably available means permitted by law and these Rules; or

(2) prejudice or damage the client during the course of the representation except as permitted or required by these Rules.

RULE 1.2.

Scope of Representation and Allocation of Authority Between Client and Lawyer

(a) Subject to the provisions herein, a lawyer shall abide by a client's decisions concerning the objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer shall abide by a client's decision whether to settle a matter. In a criminal case, the lawyer shall abide by the client's decision, after consultation with the lawyer, as to a plea to be entered, whether to waive jury trial and whether the client will testify.

(b) A lawyer's representation of a client, including representation by appointment, does not constitute an endorsement of the client's political, economic, social or moral views or activities.

(c) A lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances, the client gives informed consent and where necessary notice is provided to the tribunal and/or opposing counsel.

(d) A lawyer shall not counsel a client to engage, or assist a client, in conduct that the lawyer knows is illegal or fraudulent, except that the lawyer may discuss the legal consequences of any proposed course of conduct with a client.

(e) A lawyer may exercise professional judgment to waive or fail to assert a right or position of the client, or accede to reasonable requests of opposing counsel, when doing so does not prejudice the rights of the client.

(f) A lawyer may refuse to aid or participate in conduct that the lawyer believes to be unlawful, even though there is some support for an argument that the conduct is legal.

(g) A lawyer does not violate these Rules by being punctual in fulfilling all professional commitments, by avoiding offensive tactics, and by treating with courtesy and consideration all persons involved in the legal process.

RULE 1.3.

Diligence

(a) A lawyer shall act with reasonable diligence and promptness in representing a client.

(b) A lawyer shall not neglect a legal matter entrusted to the lawyer.

(c) A lawyer shall not intentionally fail to carry out a contract of employment entered into with a client for professional services, but the lawyer may withdraw as permitted under these Rules.

RULE 1.4.

Communication

(a) A lawyer shall:

(1) promptly inform the client of:

(i) any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(j), is required by these Rules;

(ii) any information required by court rule or other law to be communicated to a client; and

(iii) material developments in the matter including settlement or plea offers.

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with a client's reasonable requests for information; and

(5) consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by these Rules or other law.

(b) A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

RULE 1.5.

Fees and Division of Fees

(a) A lawyer shall not make an agreement for, charge, or collect an excessive or illegal fee or expense. A fee is excessive when, after a review of the facts, a reasonable lawyer would be left with a definite and firm conviction that the fee is excessive. The factors to be considered in determining whether a fee is excessive may include the following:

(1) the time and labor required, the novelty and difficulty of the questions involved, and the skill requisite to perform the legal service properly;

(2) the likelihood, if apparent or made known to the client, that the acceptance of the particular employment will preclude other employment by the lawyer;

(3) the fee customarily charged in the locality for similar legal services;

(4) the amount involved and the results obtained;

(5) the time limitations imposed by the client or by circumstances;

(6) the nature and length of the professional relationship with the client;

(7) the experience, reputation and ability of the lawyer or lawyers performing the services; and

(8) whether the fee is fixed or contingent.

(b) A lawyer shall communicate to a client the scope of the representation and the basis or rate of the fee and expenses for which the client will be responsible. This information shall be communicated to the client before or within a reasonable time after commencement of the representation and shall be in writing where required by statute or court rule. This provision shall not apply when the lawyer will charge a regularly represented client on the same basis or rate and perform services that are of the same general kind as previously rendered to and paid for by the client. Any changes in the scope of the representation or the basis or rate of the fee or expenses shall also be communicated to the client.

(c) A fee may be contingent on the outcome of the matter for which the service is rendered, except in a matter in which a contingent fee is prohibited by paragraph (d) or other law. Promptly after a lawyer has been employed in a contingent fee matter, the lawyer shall provide the client with a writing stating the method by which the fee is to be determined, including the percentage or percentages that shall accrue to the lawyer in the event of settlement, trial or appeal; litigation and other expenses to be deducted from the recovery; and whether such expenses are to be deducted before or, if not prohibited by statute or court rule, after the contingent fee is calculated. The writing must clearly notify the client of any expenses for which the client will be liable regardless of whether the client is the prevailing party. Upon conclusion of a contingent fee matter, the lawyer shall provide the client with a writing stating the outcome of the matter and, if there is a recovery, showing the remittance to the client and the method of its determination.

(d) A lawyer shall not enter into an arrangement for, charge or collect:

(1) a contingent fee for representing a defendant in a criminal matter;

(2) a fee prohibited by law or rule of court;

(3) fee based on fraudulent billing;

(4) a nonrefundable retainer fee; provided that a lawyer may enter into a retainer agreement with a client containing a reasonable minimum fee clause if it defines in plain language and sets forth the circumstances under which such fee may be incurred and how it will be calculated; or

(5) any fee in a domestic relations matter if:

(i) the payment or amount of the fee is contingent upon the securing of a divorce or of obtaining child custody or visitation or is in any way determined by reference to the amount of maintenance, support, equitable distribution, or property settlement;

(ii) a written retainer agreement has not been signed by the lawyer and client setting forth in plain language the nature of the relationship and the details of the fee arrangement; or

(iii) the written retainer agreement includes a security interest, confession of judgment or other lien without prior notice being provided to the client in a signed retainer agreement and approval from a tribunal after notice to the adversary. A lawyer shall not foreclose on a mortgage placed on the marital residence while the spouse who consents to the mortgage remains the titleholder and the residence remains the spouse's primary residence.

(e) In domestic relations matters, a lawyer shall provide a prospective client with a statement of client's rights and responsibilities at the initial conference and prior to the signing of a written retainer agreement.

(f) Where applicable, a lawyer shall resolve fee disputes by arbitration at the election of the client pursuant to a fee arbitration program established by the Chief Administrator of the Courts and approved by the Administrative Board of the Courts.

(g) A lawyer shall not divide a fee for legal services with another lawyer who is not associated in the same law firm unless:

(1) the division is in proportion to the services performed by each lawyer or, by a writing given to the client, each lawyer assumes joint responsibility for the representation;

(2) the client agrees to employment of the other lawyer after a full disclosure that a division of fees will be made, including the share each lawyer will receive, and the client's agreement is confirmed in writing; and

(3) the total fee is not excessive.

(h) Rule 1.5(g) does not prohibit payment to a lawyer formerly associated in a law firm pursuant to a separation or retirement agreement.

RULE 1.6.

Confidentiality of Information

(a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:

(1) the client gives informed consent, as defined in Rule 1.0(j);

(2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or

(3) the disclosure is permitted by paragraph (b).

"Confidential information" consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. "Confidential information" does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

(b) A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime;

(3) to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;

(4) to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer's firm or the law firm;

(5) (i) to defend the lawyer or the lawyer's employees and associates against an accusation of wrongful conduct; or

(ii) to establish or collect a fee; or

(6) when permitted or required under these Rules or to comply with other law or court order.

(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).

RULE 1.7.

Conflict of Interest: Current Clients

(a) Except as provided in paragraph (b), a lawyer shall not represent a client if a reasonable lawyer would conclude that either:

(1) the representation will involve the lawyer in representing differing interests; or

(2) there is a significant risk that the lawyer's professional judgment on behalf of a client will be adversely affected by the lawyer's own financial, business, property or other personal interests.

(b) Notwithstanding the existence of a concurrent conflict of interest under paragraph (a), a lawyer may represent a client if:

(1) the lawyer reasonably believes that the lawyer will be able to provide competent and diligent representation to each affected client;

(2) the representation is not prohibited by law;

(3) the representation does not involve the assertion of a claim by one client against another client represented by the lawyer in the same litigation or other proceeding before a tribunal; and

(4) each affected client gives informed consent, confirmed in writing.

RULE 1.8.

Current Clients: Specific Conflict of Interest Rules

(a) A lawyer shall not enter into a business transaction with a client if they have differing interests therein and if the client expects the lawyer to exercise professional judgment therein for the protection of the client, unless:

(1) the transaction is fair and reasonable to the client and the terms of the transaction are fully disclosed and transmitted in writing in a manner that can be reasonably understood by the client;

(2) the client is advised in writing of the desirability of seeking, and is given a reasonable opportunity to seek, the advice of independent legal counsel on the transaction; and

(3) the client gives informed consent, in a writing signed by the client, to the essential terms of the transaction and the lawyer's role in the transaction, including

whether the lawyer is representing the client in the transaction.

(b) A lawyer shall not use information relating to representation of a client to the disadvantage of the client unless the client gives informed consent, except as permitted or required by these Rules.

(c) A lawyer shall not:

(1) solicit any gift from a client, including a testamentary gift, for the benefit of the lawyer or a person related to the lawyer; or

(2) prepare on behalf of a client an instrument giving the lawyer or a person related to the lawyer any gift, unless the lawyer or other recipient of the gift is related to the client and a reasonable lawyer would conclude that the transaction is fair and reasonable.

For purposes of this paragraph, related persons include a spouse, child, grandchild, parent, grandparent or other relative or individual with whom the lawyer or the client maintains a close, familial relationship.

(d) Prior to conclusion of all aspects of the matter giving rise to the representation or proposed representation of the client or prospective client, a lawyer shall not negotiate or enter into any arrangement or understanding with:

(1) a client or a prospective client by which the lawyer acquires an interest in literary or media rights with respect to the subject matter of the representation or proposed representation; or

(2) any person by which the lawyer transfers or assigns any interest in literary or media rights with respect to the subject matter of the representation of a client or prospective client.

(e) While representing a client in connection with contemplated or pending litigation, a lawyer shall not advance or guarantee financial assistance to the client, except that:

(1) a lawyer may advance court costs and expenses of litigation, the repayment of which may be contingent on the outcome of the matter;

(2) a lawyer representing an indigent or pro bono client may pay court costs and expenses of litigation on behalf of the client; and

(3) a lawyer, in an action in which an attorney's fee is payable in whole or in part as a percentage of the recovery in the action, may pay on the lawyer's own account court costs and expenses of litigation. In such case, the fee paid to the lawyer from the proceeds of the action may include an amount equal to such costs and expenses incurred.

(f) A lawyer shall not accept compensation for representing a client, or anything of value related to the lawyer's representation of the client, from one other than the client unless:

(1) the client gives informed consent;

(2) there is no interference with the lawyer's independent professional judgment or with the client-lawyer relationship; and

(3) the client's confidential information is protected as required by Rule 1.6.

(g) A lawyer who represents two or more clients shall not participate in making an aggregate settlement of the claims of or against the clients, absent court approval, unless each client gives informed consent in a writing signed by the client. The lawyer's disclosure shall include the existence and nature of all the claims involved and of the participation of each person in the settlement.

(h) A lawyer shall not:

(1) make an agreement prospectively limiting the lawyer's liability to a client for malpractice; or

(2) settle a claim or potential claim for such liability with an unrepresented client or former client unless that person is advised in writing of the desirability of seeking, and is given a reasonable opportunity to seek, the advice of independent legal counsel in connection therewith.

(i) A lawyer shall not acquire a proprietary interest in the cause of action or subject matter of litigation the lawyer is conducting for a client, except that the lawyer may:

(1) acquire a lien authorized by law to secure the lawyer's fee or expenses; and

(2) contract with a client for a reasonable contingent fee in a civil matter subject to Rule 1.5(d) or other law or court rule.

(j) *(1)* A lawyer shall not:

(i) as a condition of entering into or continuing any professional representation by the lawyer or the lawyer's firm, require or demand sexual relations with any person;

(ii) employ coercion, intimidation or undue influence in entering into sexual relations incident to any professional representation by the lawyer or the lawyer's firm; or

(iii) in domestic relations matters, enter into sexual relations with a client during the course of the lawyer's representation of the client.

(2) Rule 1.8(j)(1) shall not apply to sexual relations between lawyers and their spouses or to ongoing consensual sexual relationships that predate the initiation of the client-lawyer relationship.

(k) Where a lawyer in a firm has sexual relations with a client but does not participate in the representation of that client, the lawyers in the firm shall not be subject to discipline under this Rule solely because of the occurrence of such sexual relations.

RULE 1.9.

Duties to Former Clients

(a) A lawyer who has formerly represented a client in a matter shall not thereafter represent another person in the same or a substantially related matter in

which that person's interests are materially adverse to the interests of the former client unless the former client gives informed consent, confirmed in writing.

(b) Unless the former client gives informed consent, confirmed in writing, a lawyer shall not knowingly represent a person in the same or a substantially related matter in which a firm with which the lawyer formerly was associated had previously represented a client:

(1) whose interests are materially adverse to that person; and

(2) about whom the lawyer had acquired information protected by Rules 1.6 or paragraph (c) of this Rule that is material to the matter.

(c) A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter shall not thereafter:

(1) use confidential information of the former client protected by Rule 1.6 to the disadvantage of the former client, except as these Rules would permit or require with respect to a current client or when the information has become generally known; or

(2) reveal confidential information of the former client protected by Rule 1.6 except as these Rules would permit or require with respect to a current client.

RULE 1.10.

Imputation of Conflicts of Interest

(a) While lawyers are associated in a firm, none of them shall knowingly represent a client when any one of them practicing alone would be prohibited from doing so by Rule 1.7, 1.8 or 1.9, except as otherwise provided therein.

(b) When a lawyer has terminated an association with a firm, the firm is prohibited from thereafter representing a person with interests that the firm knows or reasonably should know are materially adverse to those of a client represented by the formerly associated lawyer and not currently represented by the firm if the firm or any lawyer remaining in the firm has information protected by Rule 1.6 or Rule 1.9(c) that is material to the matter.

(c) When a lawyer becomes associated with a firm, the firm may not knowingly represent a client in a matter that is the same as or substantially related to a matter in which the newly associated lawyer, or a firm with which that lawyer was associated, formerly represented a client whose interests are materially adverse to the prospective or current client unless the newly associated lawyer did not acquire any information protected by Rule 1.6 or Rule 1.9(c) that is material to the current matter.

(d) A disqualification prescribed by this Rule may be waived by the affected client or former client under the conditions stated in Rule 1.7.

(e) A law firm shall make a written record of its engagements, at or near the time of each new engagement, and shall implement and maintain a system by which proposed engagements are checked against current and previous engagements when:

(1) the firm agrees to represent a new client;

(2) the firm agrees to represent an existing client in a new matter;

(3) the firm hires or associates with another lawyer; or

(4) an additional party is named or appears in a pending matter.

(f) Substantial failure to keep records or to implement or maintain a conflict-checking system that complies with paragraph (e) shall be a violation thereof regardless of whether there is another violation of these Rules.

(g) Where a violation of paragraph (e) by a law firm is a substantial factor in causing a violation of paragraph (a) by a lawyer, the law firm, as well as the individual lawyer, shall be responsible for the violation of paragraph (a).

(h) A lawyer related to another lawyer as parent, child, sibling or spouse shall not represent in any matter a client whose interests differ from those of another party to the matter who the lawyer knows is represented by the other lawyer unless the client consents to the representation after full disclosure and the lawyer concludes that the lawyer can adequately represent the interests of the client.

RULE 1.11.

Special Conflicts of Interest for Former and Current Government Officers and Employees

(a) Except as law may otherwise expressly provide, a lawyer who has formerly served as a public officer or employee of the government:

(1) shall comply with Rule 1.9(c); and

(2) shall not represent a client in connection with a matter in which the lawyer participated personally and substantially as a public officer or employee, unless the appropriate government agency gives its informed consent, confirmed in writing, to the representation. This provision shall not apply to matters governed by Rule 1.12(a).

(b) When a lawyer is disqualified from representation under paragraph (a), no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter unless:

(1) the firm acts promptly and reasonably to:

(i) notify, as appropriate, lawyers and nonlawyer personnel within the firm that the personally disqualified lawyer is prohibited from participating in the representation of the current client;

(ii) implement effective screening procedures to prevent the flow of information about the matter between the personally disqualified lawyer and the others in the firm;

(iii) ensure that the disqualified lawyer is apportioned no part of the fee therefrom; and

(iv) give written notice to the appropriate government agency to enable it to ascertain compliance with the provisions of this Rule; and

(2) there are no other circumstances in the particular representation that create an appearance of impropriety.

(c) Except as law may otherwise expressly provide, a lawyer having information that the lawyer knows is confidential government information about a person, acquired when the lawyer was a public officer or employee, may not represent a private client whose interests are adverse to that person in a matter in which the information could be used to the material disadvantage of that person. As used in this Rule, the term "confidential government information" means information that has been obtained under governmental authority and that, at the time this Rule is applied, the government is prohibited by law from disclosing to the public or has a legal privilege not to disclose, and that is not otherwise available to the public. A firm with which that lawyer is associated may undertake or continue representation in the matter only if the disqualified lawyer is timely and effectively screened from any participation in the matter in accordance with the provisions of paragraph (b).

(d) Except as law may otherwise expressly provide, a lawyer currently serving as a public officer or employee shall not:

(1) participate in a matter in which the lawyer participated personally and substantially while in private practice or nongovernmental employment, unless under applicable law no one is, or by lawful delegation may be, authorized to act in the lawyer's stead in the matter; or

(2) negotiate for private employment with any person who is involved as a party or as lawyer for a party in a matter in which the lawyer is participating personally and substantially.

(e) As used in this Rule, the term "matter" as defined in Rule 1.0(l) does not include or apply to agency rulemaking functions.

(f) A lawyer who holds public office shall not:

(1) use the public position to obtain, or attempt to obtain, a special advantage in legislative matters for the lawyer or for a client under circumstances where the lawyer knows or it is obvious that such action is not in the public interest;

(2) use the public position to influence, or attempt to influence, a tribunal to act in favor of the lawyer or of a client; or

(3) accept anything of value from any person when the lawyer knows or it is obvious that the offer is for the purpose of influencing the lawyer's action as a public official.

RULE 1.12.

Specific Conflicts of Interest for Former Judges, Arbitrators, Mediators or Other Third-Party Neutrals

(a) A lawyer shall not accept private employment in a matter upon the merits of which the lawyer has acted in a judicial capacity.

(b) Except as stated in paragraph (e), and unless all parties to the proceeding give informed consent, confirmed in writing, a lawyer shall not represent anyone in connection with a matter in which the lawyer participated personally and substantially as:

(1) an arbitrator, mediator or other third-party neutral; or

(2) a law clerk to a judge or other adjudicative officer or an arbitrator, mediator or other third-party neutral.

(c) A lawyer shall not negotiate for employment with any person who is involved as a party or as lawyer for a party in a matter in which the lawyer is participating personally and substantially as a judge or other adjudicative officer or as an arbitrator, mediator or other third-party neutral.

(d) When a lawyer is disqualified from representation under this Rule, no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter unless:

(1) the firm acts promptly and reasonably to:

(i) notify, as appropriate, lawyers and nonlawyer personnel within the firm that the personally disqualified lawyer is prohibited from participating in the representation of the current client;

(ii) implement effective screening procedures to prevent the flow of information about the matter between the personally disqualified lawyer and the others in the firm;

(iii) ensure that the disqualified lawyer is apportioned no part of the fee therefrom; and

(iv) give written notice to the parties and any appropriate tribunal to enable it to ascertain compliance with the provisions of this Rule; and

(2) there are no other circumstances in the particular representation that create an appearance of impropriety.

(e) An arbitrator selected as a partisan of a party in a multimember arbitration panel is not prohibited from subsequently representing that party.

RULE 1.13.

Organization As Client

(a) When a lawyer employed or retained by an organization is dealing with the organization's directors, officers, employees, members, shareholders or other constituents, and it appears that the organization's interests may differ from those of the constituents with whom the lawyer is dealing, the lawyer shall explain that the lawyer is the lawyer for the organization and not for any of the constituents.

(b) If a lawyer for an organization knows that an officer, employee or other person associated with the organization is engaged in action or intends to act or refuses to act in a matter related to the representation that (i) is a violation of a legal obligation to the organization or a violation of law that reasonably might be imputed to the organization, and (ii) is likely to result in substantial injury to the organization, then the lawyer shall proceed as is reasonably necessary in the best interest of the organization. In determining how to proceed, the lawyer shall give due consideration to the seriousness of the violation and its consequences, the scope and nature of the lawyer's representation, the responsibility in the organization and the apparent motivation of the person involved, the policies of the organization concerning such matters and any other relevant considerations. Any measures taken shall be designed to minimize disruption of the organization and

the risk of revealing information relating to the representation to persons outside the organization. Such measures may include, among others:

(1) asking reconsideration of the matter;

(2) advising that a separate legal opinion on the matter be sought for presentation to an appropriate authority in the organization; and

(3) referring the matter to higher authority in the organization, including, if warranted by the seriousness of the matter, referral to the highest authority that can act in behalf of the organization as determined by applicable law.

(c) If, despite the lawyer's efforts in accordance with paragraph (b), the highest authority that can act on behalf of the organization insists upon action, or a refusal to act, that is clearly in violation of law and is likely to result in a substantial injury to the organization, the lawyer may reveal confidential information only if permitted by Rule 1.6, and may resign in accordance with Rule 1.16.

(d) A lawyer representing an organization may also represent any of its directors, officers, employees, members, shareholders or other constituents, subject to the provisions of Rule 1.7. If the organization's consent to the concurrent representation is required by Rule 1.7, the consent shall be given by an appropriate official of the organization other than the individual who is to be represented, or by the shareholders.

RULE 1.14.

Client With Diminished Capacity

(a) When a client's capacity to make adequately considered decisions in connection with a representation is diminished, whether because of minority, mental impairment or for some other reason, the lawyer shall, as far as reasonably possible, maintain a conventional relationship with the client.

(b) When the lawyer reasonably believes that the client has diminished capacity, is at risk of substantial physical, financial or other harm unless action is taken and cannot adequately act in the client's own interest, the lawyer may take reasonably necessary protective action, including consulting with individuals or entities that have the ability to take action to protect the client and, in appropriate cases, seeking the appointment of a guardian ad litem, conservator or guardian.

(c) Information relating to the representation of a client with diminished capacity is protected by Rule 1.6. When taking protective action pursuant to paragraph (b), the lawyer is impliedly authorized under Rule 1.6(a) to reveal information about the client, but only to the extent reasonably necessary to protect the client's interests.

RULE 1.15.

Preserving Identity of Funds and Property of Others; Fiduciary Responsibility; Commingling and Misappropriation of Client Funds or Property; Maintenance of Bank Accounts; Record Keeping; Examination of Records

(a) Prohibition Against Commingling and Misappropriation of Client Funds or Property.

> A lawyer in possession of any funds or other property belonging to another person, where such possession is incident to his or her practice of law, is a fiduciary, and must not misappropriate such funds or property or commingle such funds or property with his or her own.

(b) Separate Accounts.

> *(1)* A lawyer who is in possession of funds belonging to another person incident to the lawyer's practice of law shall maintain such funds in a banking institution within New York State that agrees to provide dishonored check reports in accordance with the provisions of 22 N.Y.C.R.R. Part 1300. "Banking institution" means a state or national bank, trust company, savings bank, savings and loan association or credit union. Such funds shall be maintained, in the lawyer's own name, or in the name of a firm of lawyers of which the lawyer is a member, or in the name of the lawyer or firm of lawyers by whom the lawyer is employed, in a special account or accounts, separate from any business or personal accounts of the lawyer or lawyer's firm, and separate from any accounts that the lawyer may maintain as executor, guardian, trustee or receiver, or in any other fiduciary capacity; into such special account or accounts all funds held in escrow or otherwise entrusted to the lawyer or firm shall be deposited; provided, however, that such funds may be maintained in a banking institution located outside New York State if such

banking institution complies with 22 N.Y.C.R.R. Part 1300 and the lawyer has obtained the prior written approval of the person to whom such funds belong specifying the name and address of the office or branch of the banking institution where such funds are to be maintained.

(2) A lawyer or the lawyer's firm shall identify the special bank account or accounts required by Rule 1.15(b)(1) as an "Attorney Special Account," "Attorney Trust Account," or "Attorney Escrow Account," and shall obtain checks and deposit slips that bear such title. Such title may be accompanied by such other descriptive language as the lawyer may deem appropriate, provided that such additional language distinguishes such special account or accounts from other bank accounts that are maintained by the lawyer or the lawyer's firm.

(3) Funds reasonably sufficient to maintain the account or to pay account charges may be deposited therein.

(4) Funds belonging in part to a client or third person and in part currently or potentially to the lawyer or law firm shall be kept in such special account or accounts, but the portion belonging to the lawyer or law firm may be withdrawn when due unless the right of the lawyer or law firm to receive it is disputed by the client or third person, in which event the disputed portion shall not be withdrawn until the dispute is finally resolved.

(c) Notification of Receipt of Property; Safekeeping; Rendering Accounts; Payment or Delivery of Property.

A lawyer shall:

(1) promptly notify a client or third person of the receipt of funds, securities, or other properties in which the client or third person has an interest;

(2) identify and label securities and properties of a client or third person promptly upon receipt and place them

in a safe deposit box or other place of safekeeping as soon as practicable;

(3) maintain complete records of all funds, securities, and other properties of a client or third person coming into the possession of the lawyer and render appropriate accounts to the client or third person regarding them; and

(4) promptly pay or deliver to the client or third person as requested by the client or third person the funds, securities, or other properties in the possession of the lawyer that the client or third person is entitled to receive.

(d) Required Bookkeeping Records.

(1) A lawyer shall maintain for seven years after the events that they record:

(i) the records of all deposits in and withdrawals from the accounts specified in Rule 1.15(b) and of any other bank account that concerns or affects the lawyer's practice of law; these records shall specifically identify the date, source and description of each item deposited, as well as the date, payee and purpose of each withdrawal or disbursement;

(ii) a record for special accounts, showing the source of all funds deposited in such accounts, the names of all persons for whom the funds are or were held, the amount of such funds, the description and amounts, and the names of all persons to whom such funds were disbursed;

(iii) copies of all retainer and compensation agreements with clients;

(iv) copies of all statements to clients or other persons showing the disbursement of funds to them or on their behalf;

(v) copies of all bills rendered to clients;

(vi) copies of all records showing payments to lawyers, investigators or other persons, not in the lawyer's regular employ, for services rendered or performed;

(vii) copies of all retainer and closing statements filed with the Office of Court Administration; and

(viii) all checkbooks and check stubs, bank statements, prenumbered canceled checks and duplicate deposit slips.

(2) Lawyers shall make accurate entries of all financial transactions in their records of receipts and disbursements, in their special accounts, in their ledger books or similar records, and in any other books of account kept by them in the regular course of their practice, which entries shall be made at or near the time of the act, condition or event recorded.

(3) For purposes of Rule 1.15(d), a lawyer may satisfy the requirements of maintaining "copies" by maintaining any of the following items: original records, photocopies, microfilm, optical imaging, and any other medium that preserves an image of the document that cannot be altered without detection.

(e) Authorized Signatories.

All special account withdrawals shall be made only to a named payee and not to cash. Such withdrawals shall be made by check or, with the prior written approval of the party entitled to the proceeds, by bank transfer. Only a lawyer admitted to practice law in New York State shall be an authorized signatory of a special account.

(f) Missing Clients.

Whenever any sum of money is payable to a client and the lawyer is unable to locate the client, the lawyer shall apply to the court in which the action was brought if in the unified court system, or, if no action was commenced in the unified court system, to the Supreme Court in the county in which the lawyer maintains an

office for the practice of law, for an order directing payment to the lawyer of any fees and disbursements that are owed by the client and the balance, if any, to the Lawyers' Fund for Client Protection for safeguarding and disbursement to persons who are entitled thereto.

(g) Designation of Successor Signatories.

(1) Upon the death of a lawyer who was the sole signatory on an attorney trust, escrow or special account, an application may be made to the Supreme Court for an order designating a successor signatory for such trust, escrow or special account, who shall be a member of the bar in good standing and admitted to the practice of law in New York State.

(2) An application to designate a successor signatory shall be made to the Supreme Court in the judicial district in which the deceased lawyer maintained an office for the practice of law. The application may be made by the legal representative of the deceased lawyer's estate; a lawyer who was affiliated with the deceased lawyer in the practice of law; any person who has a beneficial interest in such trust, escrow or special account; an officer of a city or county bar association; or counsel for an attorney disciplinary committee. No lawyer may charge a legal fee for assisting with an application to designate a successor signatory pursuant to this Rule.

(3) The Supreme Court may designate a successor signatory and may direct the safeguarding of funds from such trust, escrow or special account, and the disbursement of such funds to persons who are entitled thereto, and may order that funds in such account be deposited with the Lawyers' Fund for Client Protection for safeguarding and disbursement to persons who are entitled thereto.

(h) Dissolution of a Firm.

Upon the dissolution of any firm of lawyers, the former partners or members shall make appropriate arrangements for the maintenance, by one of them or by a successor firm, of the records specified in Rule 1.15(d).

(i) Availability of Bookkeeping Records: Records Subject to Production in Disciplinary Investigations and Proceedings.

The financial records required by this Rule shall be located, or made available, at the principal New York State office of the lawyers subject hereto, and any such records shall be produced in response to a notice or subpoena duces tecum issued in connection with a complaint before or any investigation by the appropriate grievance or departmental disciplinary committee, or shall be produced at the direction of the appropriate Appellate Division before any person designated by it. All books and records produced pursuant to this Rule shall be kept confidential, except for the purpose of the particular proceeding, and their contents shall not be disclosed by anyone in violation of the attorney-client privilege.

(j) Disciplinary Action.

A lawyer who does not maintain and keep the accounts and records as specified and required by this Rule, or who does not produce any such records pursuant to this Rule, shall be deemed in violation of these Rules and shall be subject to disciplinary proceedings.

RULE 1.16.

Declining or Terminating Representation

(a) A lawyer shall not accept employment on behalf of a person if the lawyer knows or reasonably should know that such person wishes to:

(1) bring a legal action, conduct a defense, or assert a position in a matter, or otherwise have steps taken for such person, merely for the purpose of harassing or maliciously injuring any person; or

(2) present a claim or defense in a matter that is not warranted under existing law, unless it can be supported by a good faith argument for an extension, modification, or reversal of existing law.

(b) Except as stated in paragraph (d), a lawyer shall withdraw from the representation of a client when:

(1) the lawyer knows or reasonably should know that the representation will result in a violation of these Rules or of law;

(2) the lawyer's physical or mental condition materially impairs the lawyer's ability to represent the client;

(3) the lawyer is discharged; or

(4) the lawyer knows or reasonably should know that the client is bringing the legal action, conducting the defense, or asserting a position in the matter, or is otherwise having steps taken, merely for the purpose of harassing or maliciously injuring any person.

(c) Except as stated in paragraph (d), a lawyer may withdraw from representing a client when:

(1) withdrawal can be accomplished without material adverse effect on the interests of the client;

(2) the client persists in a course of action involving the lawyer's services that the lawyer reasonably believes is criminal or fraudulent;

(3) the client has used the lawyer's services to perpetrate a crime or fraud;

(4) the client insists upon taking action with which the lawyer has a fundamental disagreement;

(5) the client deliberately disregards an agreement or obligation to the lawyer as to expenses or fees;

(6) the client insists upon presenting a claim or defense that is not warranted under existing law and cannot be supported by good faith argument for an extension, modification, or reversal of existing law;

(7) the client fails to cooperate in the representation or otherwise renders the representation unreasonably difficult for the lawyer to carry out employment effectively;

(8) the lawyer's inability to work with co-counsel indicates that the best interest of the client likely will be served by withdrawal;

(9) the lawyer's mental or physical condition renders it difficult for the lawyer to carry out the representation effectively;

(10) the client knowingly and freely assents to termination of the employment;

(11) withdrawal is permitted under Rule 1.13(c) or other law;

(12) the lawyer believes in good faith, in a matter pending before a tribunal, that the tribunal will find the existence of other good cause for withdrawal; or

(13) the client insists that the lawyer pursue a course of conduct which is illegal or prohibited under these Rules.

(d) If permission for withdrawal from employment is required by the rules of a tribunal, a lawyer shall not withdraw from employment in a matter before that tribunal without its permission. When ordered to do so by a tribunal, a lawyer shall continue representation notwithstanding good cause for terminating the representation.

(e) Even when withdrawal is otherwise permitted or required, upon termination of representation, a lawyer shall take steps, to the extent reasonably practicable, to avoid foreseeable prejudice to the rights of the client, including giving reasonable notice to the client, allowing time for employment of other counsel, delivering to the client all papers and property to which the client is entitled, promptly refunding any part of a fee paid in advance that has not been earned and complying with applicable laws and rules.

RULE 1.17.

Sale of Law Practice

(a) A lawyer retiring from a private practice of law; a law firm, one or more members of which are retiring from the private practice of law with the firm; or the personal representative of a deceased, disabled or missing lawyer, may sell a law practice, including goodwill, to one or more lawyers or law firms, who may purchase the practice. The seller and the buyer may agree on reasonable restrictions on the seller's private practice of law, notwithstanding any other provision of these Rules. Retirement shall include the cessation of the private

practice of law in the geographic area, that is, the county and city and any county or city contiguous thereto, in which the practice to be sold has been conducted.

(b) Confidential information.

(1) With respect to each matter subject to the contemplated sale, the seller may provide prospective buyers with any information not protected as confidential information under Rule 1.6.

(2) Notwithstanding Rule 1.6, the seller may provide the prospective buyer with information as to individual clients:

(i) concerning the identity of the client, except as provided in paragraph (b)(6);

(ii) concerning the status and general nature of the matter;

(iii) available in public court files; and

(iv) concerning the financial terms of the client-lawyer relationship and the payment status of the client's account.

(3) Prior to making any disclosure of confidential information that may be permitted under paragraph (b)(2), the seller shall provide the prospective buyer with information regarding the matters involved in the proposed sale sufficient to enable the prospective buyer to determine whether any conflicts of interest exist. Where sufficient information cannot be disclosed without revealing client confidential information, the seller may make the disclosures necessary for the prospective buyer to determine whether any conflict of interest exists, subject to paragraph (b)(6). If the prospective buyer determines that conflicts of interest exist prior to reviewing the information, or determines during the course of review that a conflict of interest exists, the prospective buyer shall not review or continue to review the information unless the seller shall have

obtained the consent of the client in accordance with Rule 1.6(a)(1).

(4) Prospective buyers shall maintain the confidentiality of and shall not use any client information received in connection with the proposed sale in the same manner and to the same extent as if the prospective buyers represented the client.

(5) Absent the consent of the client after full disclosure, a seller shall not provide a prospective buyer with information if doing so would cause a violation of the attorney-client privilege.

(6) If the seller has reason to believe that the identity of the client or the fact of the representation itself constitutes confidential information in the circumstances, the seller may not provide such information to a prospective buyer without first advising the client of the identity of the prospective buyer and obtaining the client's consent to the proposed disclosure.

(c) Written notice of the sale shall be given jointly by the seller and the buyer to each of the seller's clients and shall include information regarding:

(1) the client's right to retain other counsel or to take possession of the file;

(2) the fact that the client's consent to the transfer of the client's file or matter to the buyer will be presumed if the client does not take any action or otherwise object within 90 days of the sending of the notice, subject to any court rule or statute requiring express approval by the client or a court;

(3) the fact that agreements between the seller and the seller's clients as to fees will be honored by the buyer;

(4) proposed fee increases, if any, permitted under paragraph (e); and

(5) the identity and background of the buyer or buyers, including principal office address, bar admissions,

number of years in practice in New York State, whether the buyer has ever been disciplined for professional misconduct or convicted of a crime, and whether the buyer currently intends to resell the practice.

(d) When the buyer's representation of a client of the seller would give rise to a waivable conflict of interest, the buyer shall not undertake such representation unless the necessary waiver or waivers have been obtained in writing.

(e) The fee charged a client by the buyer shall not be increased by reason of the sale, unless permitted by a retainer agreement with the client or otherwise specifically agreed to by the client.

RULE 1.18.

Duties to Prospective Clients

(a) Except as provided in Rule l.18(e), a person who consults with a lawyer about the possibility of forming a client-lawyer relationship with respect to a matter is a prospective client.

(b) Even when no client-lawyer relationship ensues, a lawyer who has learned information from a prospective client shall not use or reveal that information, except as Rule 1.9 would permit with respect to information of a former client.

(c) A lawyer subject to paragraph (b) shall not represent a client with interests materially adverse to those of a prospective client in the same or a substantially related matter if the lawyer received information from the prospective client that could be significantly harmful to that person in the matter, except as provided in paragraph (d). If a lawyer is disqualified from representation under this paragraph, no lawyer in a firm with which that lawyer is associated may knowingly undertake or continue representation in such a matter, except as provided in paragraph (d).

(d) When the lawyer has received disqualifying information as defined in paragraph (c), representation is permissible if:

(1) both the affected client and the prospective client have given informed consent, confirmed in writing; or

(2) the lawyer who received the information took reasonable measures to avoid exposure to more

disqualifying information than was reasonably necessary to determine whether to represent the prospective client; and

(i) the firm acts promptly and reasonably to notify, as appropriate, lawyers and nonlawyer personnel within the firm that the personally disqualified lawyer is prohibited from participating in the representation of the current client;

(ii) the firm implements effective screening procedures to prevent the flow of information about the matter between the disqualified lawyer and the others in the firm;

(iii) the disqualified lawyer is apportioned no part of the fee therefrom; and

(iv) written notice is promptly given to the prospective client; and

(3) a reasonable lawyer would conclude that the law firm will be able to provide competent and diligent representation in the matter.

(e) A person is not a prospective client within the meaning of paragraph (a) if the person:

(1) communicates information unilaterally to a lawyer, without any reasonable expectation that the lawyer is willing to discuss the possibility of forming a client-lawyer relationship; or

(2) communicates with a lawyer for the purpose of disqualifying the lawyer from handling a materially adverse representation on the same or a substantially related matter.

RULE 2.1.

Advisor

In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social, psychological, and political factors that may be relevant to the client's situation.

RULE 2.2.

[Reserved]

RULE 2.3.

Evaluation for Use by Third Persons

(a) A lawyer may provide an evaluation of a matter affecting a client for the use of someone other than the client if the lawyer reasonably believes that making the evaluation is compatible with other aspects of the lawyer's relationship with the client.

(b) When the lawyer knows or reasonably should know that the evaluation is likely to affect the client's interests materially and adversely, the lawyer shall not provide the evaluation unless the client gives informed consent.

(c) Unless disclosure is authorized in connection with a report of an evaluation, information relating to the evaluation is protected by Rule 1.6.

RULE 2.4.

Lawyer Serving as Third-Party Neutral

(a) A lawyer serves as a "third-party neutral" when the lawyer assists two or more persons who are not clients of the lawyer to reach a resolution of a dispute or other matter that has arisen between them. Service as a third-party neutral may include service as an arbitrator, a mediator or in such other capacity as will enable the lawyer to assist the parties to resolve the matter.

(b) A lawyer serving as a third-party neutral shall inform unrepresented parties that the lawyer is not representing them. When the lawyer knows or

reasonably should know that a party does not understand the lawyer's role in the matter, the lawyer shall explain the difference between the lawyer's role as a third-party neutral and a lawyer's role as one who represents a client.

RULE 3.1.

Non-Meritorious Claims and Contentions

(a) A lawyer shall not bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis in law and fact for doing so that is not frivolous. A lawyer for the defendant in a criminal proceeding or for the respondent in a proceeding that could result in incarceration may nevertheless so defend the proceeding as to require that every element of the case be established.

(b) A lawyer's conduct is "frivolous" for purposes of this Rule if:

(1) the lawyer knowingly advances a claim or defense that is unwarranted under existing law, except that the lawyer may advance such claim or defense if it can be supported by good faith argument for an extension, modification, or reversal of existing law;

(2) the conduct has no reasonable purpose other than to delay or prolong the resolution of litigation, in violation of Rule 3.2, or serves merely to harass or maliciously injure another; or

(3) the lawyer knowingly asserts material factual statements that are false.

RULE 3.2.

Delay of Litigation

In representing a client, a lawyer shall not use means that have no substantial purpose other than to delay or prolong the proceeding or to cause needless expense.

RULE 3.3.

Conduct Before a Tribunal

(a) A lawyer shall not knowingly:

(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;

(2) fail to disclose to the tribunal controlling legal authority known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or

(3) offer or use evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.

(b) A lawyer who represents a client before a tribunal and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties stated in paragraphs (a) and (b) apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.

(d) In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision, whether or not the facts are adverse.

(e) In presenting a matter to a tribunal, a lawyer shall disclose, unless privileged or irrelevant, the identities of the clients the lawyer represents and of the persons who employed the lawyer.

(f) In appearing as a lawyer before a tribunal, a lawyer shall not:

(1) fail to comply with known local customs of courtesy or practice of the bar or a particular tribunal without giving to opposing counsel timely notice of the intent not to comply;

(2) engage in undignified or discourteous conduct;

(3) intentionally or habitually violate any established rule of procedure or of evidence; or

(4) engage in conduct intended to disrupt the tribunal.

RULE 3.4.

Fairness to Opposing Party and Counsel

A lawyer shall not:

(a) *(1)* suppress any evidence that the lawyer or the client has a legal obligation to reveal or produce;

(2) advise or cause a person to hide or leave the jurisdiction of a tribunal for the purpose of making the person unavailable as a witness therein;

(3) conceal or knowingly fail to disclose that which the lawyer is required by law to reveal;

(4) knowingly use perjured testimony or false evidence;

(5) participate in the creation or preservation of evidence when the lawyer knows or it is obvious that the evidence is false; or

(6) knowingly engage in other illegal conduct or conduct contrary to these Rules;

(b) offer an inducement to a witness that is prohibited by law or pay, offer to pay or acquiesce in the payment of compensation to a witness contingent upon the content of the witness's testimony or the outcome of the matter. A lawyer may advance, guarantee or acquiesce in the payment of:

(1) reasonable compensation to a witness for the loss of time in attending, testifying, preparing to testify or otherwise assisting counsel, and reasonable related expenses; or

(2) a reasonable fee for the professional services of an expert witness and reasonable related expenses;

(c) disregard or advise the client to disregard a standing rule of a tribunal or a ruling of a tribunal made in the course of a proceeding, but the lawyer may take appropriate steps in good faith to test the validity of such rule or ruling;

(d) in appearing before a tribunal on behalf of a client:

(1) state or allude to any matter that the lawyer does not reasonably believe is relevant or that will not be supported by admissible evidence;

(2) assert personal knowledge of facts in issue except when testifying as a witness;

(3) assert a personal opinion as to the justness of a cause, the credibility of a witness, the culpability of a civil litigant or the guilt or innocence of an accused but the lawyer may argue, upon analysis of the evidence, for any position or conclusion with respect to the matters stated herein; or

(4) ask any question that the lawyer has no reasonable basis to believe is relevant to the case and that is intended to degrade a witness or other person; or

(e) present, participate in presenting, or threaten to present criminal charges solely to obtain an advantage in a civil matter.

RULE 3.5.

Maintaining and Preserving the Impartiality of Tribunals and Jurors

(a) A lawyer shall not:

(1) seek to or cause another person to influence a judge, official or employee of a tribunal by means prohibited by law or give or lend anything of value to such judge, official, or employee of a tribunal when the recipient is prohibited from accepting the gift or loan but a lawyer may make a contribution to the campaign fund of a candidate for judicial office in conformity with Part 100 of the Rules of the Chief Administrator of the Courts;

(2) in an adversarial proceeding communicate or cause another person to do so on the lawyer's behalf, as to the merits of the matter with a judge or official of a tribunal or an employee thereof before whom the matter is pending, except:

(i) in the course of official proceedings in the matter;

(ii) in writing, if the lawyer promptly delivers a copy of the writing to counsel for other parties and to a party who is not represented by a lawyer;

(iii) orally, upon adequate notice to counsel for the other parties and to any party who is not represented by a lawyer; or

(iv) as otherwise authorized by law, or by Part 100 of the Rules of the Chief Administrator of the Courts;

(3) seek to or cause another person to influence a juror or prospective juror by means prohibited by law;

(4) communicate or cause another to communicate with a member of the jury venire from which the jury will be selected for the trial of a case or, during the trial of a case, with any member of the jury unless authorized to do so by law or court order;

(5) communicate with a juror or prospective juror after discharge of the jury if:

(i) the communication is prohibited by law or court order;

(ii) the juror has made known to the lawyer a desire not to communicate;

(iii) the communication involves misrepresentation, coercion, duress or harassment; or

(iv) the communication is an attempt to influence the juror's actions in future jury service; or

(6) conduct a vexatious or harassing investigation of either a member of the venire or a juror or, by financial support or otherwise, cause another to do so.

(b) During the trial of a case a lawyer who is not connected therewith shall not communicate with or cause another to communicate with a juror concerning the case.

(c) All restrictions imposed by this Rule also apply to communications with or investigations of members of a family of a member of the venire or a juror.

(d) A lawyer shall reveal promptly to the court improper conduct by a member of the venire or a juror, or by another toward a member of the venire or a juror or a member of his or her family of which the lawyer has knowledge.

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.

(b) A statement ordinarily is likely to prejudice materially an adjudicative proceeding when it refers to a civil matter triable to a jury, a criminal matter or any other proceeding that could result in incarceration, and the statement relates to:

(1) the character, credibility, reputation or criminal record of a party, suspect in a criminal investigation or witness, or the identity of a witness or the expected testimony of a party or witness;

(2) in a criminal matter that could result in incarceration, the possibility of a plea of guilty to the offense or the existence or contents of any confession, admission or statement given by a defendant or suspect, or that person's refusal or failure to make a statement;

(3) the performance or results of any examination or test, or the refusal or failure of a person to submit to an examination or test, or the identity or nature of physical evidence expected to be presented;

(4) any opinion as to the guilt or innocence of a defendant or suspect in a criminal matter that could result in incarceration;

(5) information the lawyer knows or reasonably should know is likely to be inadmissible as evidence in a trial and would, if disclosed, create a substantial risk of prejudicing an impartial trial; or

(6) the fact that a defendant has been charged with a crime, unless there is included therein a statement explaining that the charge is merely an accusation and that the defendant is presumed innocent until and unless proven guilty.

(c) Provided that the statement complies with paragraph (a), a lawyer may state the following without elaboration:

(1) the claim, offense or defense and, except when prohibited by law, the identity of the persons involved;

(2) information contained in a public record;

(3) that an investigation of a matter is in progress;

(4) the scheduling or result of any step in litigation;

(5) a request for assistance in obtaining evidence and information necessary thereto;

(6) a warning of danger concerning the behavior of a person involved, when there is reason to believe that there exists the likelihood of substantial harm to an individual or to the public interest; and

(7) in a criminal matter:

(i) the identity, age, residence, occupation and family status of the accused;

(ii) if the accused has not been apprehended, information necessary to aid in apprehension of that person;

(iii) the identity of investigating and arresting officers or agencies and the length of the investigation; and

(iv) the fact, time and place of arrest, resistance, pursuit and use of weapons, and a description of physical evidence seized, other than as contained only in a confession, admission or statement.

(d) Notwithstanding paragraph (a), a lawyer may make a statement that a reasonable lawyer would believe is required to protect a client from the substantial prejudicial effect of recent publicity not initiated by the lawyer or the lawyer's client. A statement made pursuant to this paragraph shall be limited to such information as is necessary to mitigate the recent adverse publicity.

(e) No lawyer associated in a firm or government agency with a lawyer subject to paragraph (a) shall make a statement prohibited by paragraph (a).

RULE 3.7.

Lawyer As Witness

(a) A lawyer shall not act as advocate before a tribunal in a matter in which the lawyer is likely to be a witness on a significant issue of fact unless:

(1) the testimony relates solely to an uncontested issue;

(2) the testimony relates solely to the nature and value of legal services rendered in the matter;

(3) disqualification of the lawyer would work substantial hardship on the client;

(4) the testimony will relate solely to a matter of formality, and there is no reason to believe that substantial evidence will be offered in opposition to the testimony; or

(5) the testimony is authorized by the tribunal.

(b) A lawyer may not act as advocate before a tribunal in a matter if:

(1) another lawyer in the lawyer's firm is likely to be called as a witness on a significant issue other than on behalf of the client, and it is apparent that the testimony may be prejudicial to the client; or

(2) the lawyer is precluded from doing so by Rule 1.7 or Rule 1.9.

RULE 3.8.

Special Responsibilities of Prosecutors and Other Government Lawyers

(a) A prosecutor or other government lawyer shall not institute, cause to be instituted or maintain a criminal charge when the prosecutor or other government lawyer knows or it is obvious that the charge is not supported by probable cause.

(b) A prosecutor or other government lawyer in criminal litigation shall make timely disclosure to counsel for the defendant or to a defendant who has no counsel of the existence of evidence or information known to the prosecutor or other government lawyer that tends to negate the guilt of the accused, mitigate the degree of the offense, or reduce the sentence, except when relieved of this responsibility by a protective order of a tribunal.

(c) When a prosecutor knows of new, credible and material evidence creating a reasonable likelihood that a convicted defendant did not commit an offense of which the defendant was convicted, the prosecutor shall within a reasonable time:

(1) disclose that evidence to an appropriate court or prosecutor's office; or

(2) if the conviction was obtained by that prosecutor's office,

(A) notify the appropriate court and the defendant that the prosecutor's office possesses such evidence unless a court authorizes delay for good cause shown;

(B) disclose that evidence to the defendant unless the disclosure would interfere with an ongoing investigation or endanger the safety of a witness or other person, and a court authorizes delay for good cause shown; and

(C) undertake or make reasonable efforts to cause to be undertaken such further inquiry or investigation as may be necessary to provide a reasonable belief that the conviction should or should not be set aside.

(d) When a prosecutor knows of clear and convincing evidence establishing that a defendant was convicted, in a prosecution by the prosecutor's office, of an offense that the defendant did not commit, the prosecutor shall seek a remedy consistent with justice, applicable law, and the circumstances of the case.

(e) A prosecutor's independent judgment, made in good faith, that the new evidence is not of such nature as to trigger the obligations of sections (c) and (d), though subsequently determined to have been erroneous, does not constitute a violation of this rule.

RULE 3.9.

Advocate In Non-Adjudicative Matters

A lawyer communicating in a representative capacity with a legislative body or administrative agency in connection with a pending non-adjudicative matter or proceeding shall disclose that the appearance is in a representative capacity, except when the lawyer seeks information from an agency that is available to the public.

RULE 4.1.

Truthfulness In Statements To Others

In the course of representing a client, a lawyer shall not knowingly make a false statement of fact or law to a third person.

RULE 4.2.

Communication With Person Represented By Counsel

(a) In representing a client, a lawyer shall not communicate or cause another to communicate about the subject of the representation with a party the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the prior consent of the other lawyer or is authorized to do so by law.

(b) Notwithstanding the prohibitions of paragraph (a), and unless otherwise prohibited by law, a lawyer may cause a client to communicate with a represented person unless the represented person is not legally competent, and may counsel the client with respect to those communications, provided the lawyer gives reasonable advance notice to the represented person's counsel that such communications will be taking place.

(c) A lawyer who is acting *pro se* or is represented by counsel in a matter is subject to paragraph (a), but may communicate with a represented person, unless otherwise prohibited by law and unless the represented person is not legally competent, provided the lawyer or the lawyer's counsel gives reasonable advance notice to the represented person's counsel that such communications will be taking place.

RULE 4.3.

Communicating With Unrepresented Persons

In communicating on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding. The lawyer shall not give legal advice to an unrepresented person other than the advice to secure counsel if the lawyer knows or reasonably should know that the interests of such person are or have a reasonable possibility of being in conflict with the interests of the client.

RULE 4.4.

Respect for Rights of Third Persons

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass or harm a third person or use methods of obtaining evidence that violate the legal rights of such a person.

(b) A lawyer who receives a document, electronically stored information, or other writing relating to the representation of the lawyer's client and knows or reasonably should know that it was inadvertently sent shall promptly notify the sender.

RULE 4.5.

Communication After Incidents Involving Personal Injury or Wrongful Death

(a) In the event of a specific incident involving potential claims for personal injury or wrongful death, no unsolicited communication shall be made to an individual injured in the incident or to a family member or legal representative of such an individual, by a lawyer or law firm, or by any associate, agent, employee or other representative of a lawyer or law firm representing actual or potential defendants or entities that may defend and/or indemnify said defendants, before the 30th day after the date of the incident, unless a filing must be made within 30 days of the incident as a legal prerequisite to the particular claim, in which case no unsolicited communication shall be made before the 15th day after the date of the incident.

(b) An unsolicited communication by a lawyer or law firm, seeking to represent an injured individual or the legal representative thereof under the circumstance described in paragraph (a) shall comply with Rule 7.3(e).

RULE 5.1.

Responsibilities of Law Firms, Partners, Managers and Supervisory Lawyers

(a) A law firm shall make reasonable efforts to ensure that all lawyers in the firm conform to these Rules.

(b) *(1)* A lawyer with management responsibility in a law firm shall make reasonable efforts to ensure that other lawyers in the law firm conform to these Rules.

(2) A lawyer with direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the supervised lawyer conforms to these Rules.

(c) A law firm shall ensure that the work of partners and associates is adequately supervised, as appropriate. A lawyer with direct supervisory authority over another lawyer shall adequately supervise the work of the other lawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter, and the likelihood that ethical problems might arise in the course of working on the matter.

(d) A lawyer shall be responsible for a violation of these Rules by another lawyer if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the other lawyer practices or is a lawyer who has supervisory authority over the other lawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

RULE 5.2.

Responsibilities of a Subordinate Lawyer

(a) A lawyer is bound by these Rules notwithstanding that the lawyer acted at the direction of another person.

(b) A subordinate lawyer does not violate these Rules if that lawyer acts in accordance with a supervisory lawyer's reasonable resolution of an arguable question of professional duty.

RULE 5.3.

Lawyer's Responsibility for Conduct of Nonlawyers

(a) A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate. A lawyer with direct supervisory authority over a nonlawyer shall adequately supervise the work of the nonlawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter and the likelihood that ethical problems might arise in the course of working on the matter.

(b) A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the nonlawyer is employed or is a

lawyer who has supervisory authority over the nonlawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

RULE 5.4.

Professional Independence of a Lawyer

(a) A lawyer or law firm shall not share legal fees with a nonlawyer, except that:

(1) an agreement by a lawyer with the lawyer's firm or another lawyer associated in the firm may provide for the payment of money, over a reasonable period of time after the lawyer's death, to the lawyer's estate or to one or more specified persons;

(2) a lawyer who undertakes to complete unfinished legal business of a deceased lawyer may pay to the estate of the deceased lawyer that portion of the total compensation that fairly represents the services rendered by the deceased lawyer; and

(3) a lawyer or law firm may compensate a nonlawyer employee or include a nonlawyer employee in a retirement plan based in whole or in part on a profit-sharing arrangement.

(b) A lawyer shall not form a partnership with a nonlawyer if any of the activities of the partnership consist of the practice of law.

(c) Unless authorized by law, a lawyer shall not permit a person who recommends, employs or pays the lawyer to render legal service for another to

direct or regulate the lawyer's professional judgment in rendering such legal services or to cause the lawyer to compromise the lawyer's duty to maintain the confidential information of the client under Rule 1.6.

(d) A lawyer shall not practice with or in the form of an entity authorized to practice law for profit, if:

(1) a nonlawyer owns any interest therein, except that a fiduciary representative of the estate of a lawyer may hold the stock or interest of the lawyer for a reasonable time during administration;

(2) a nonlawyer is a member, corporate director or officer thereof or occupies a position of similar responsibility in any form of association other than a corporation; or

(3) a nonlawyer has the right to direct or control the professional judgment of a lawyer.

RULE 5.5.

Unauthorized Practice of Law

(a) A lawyer shall not practice law in a jurisdiction in violation of the regulation of the legal profession in that jurisdiction.

(b) A lawyer shall not aid a nonlawyer in the unauthorized practice of law.

RULE 5.6.

Restrictions On Right To Practice

(a) A lawyer shall not participate in offering or making:

(1) a partnership, shareholder, operating, employment, or other similar type of agreement that restricts the right of a lawyer to practice after termination of the relationship, except an agreement concerning benefits upon retirement; or

(2) an agreement in which a restriction on a lawyer's right to practice is part of the settlement of a client controversy.

(b) This Rule does not prohibit restrictions that may be included in the terms of the sale of a law practice pursuant to Rule 1.17.

RULE 5.7.

Responsibilities Regarding Nonlegal Services

(a) With respect to lawyers or law firms providing nonlegal services to clients or other persons:

(1) A lawyer or law firm that provides nonlegal services to a person that are not distinct from legal services being provided to that person by the lawyer or law firm is subject to these Rules with respect to the provision of both legal and nonlegal services.

(2) A lawyer or law firm that provides nonlegal services to a person that are distinct from legal services being provided to that person by the lawyer or law firm is subject to these Rules with respect to the nonlegal services if the person receiving the services could reasonably believe that the nonlegal services are the subject of a client-lawyer relationship.

(3) A lawyer or law firm that is an owner, controlling party or agent of, or that is otherwise affiliated with, an entity that the lawyer or law firm knows to be providing nonlegal services to a person is subject to these Rules with respect to the nonlegal services if the person receiving the services could reasonably believe that the nonlegal services are the subject of a client-lawyer relationship.

(4) For purposes of paragraphs (a)(2) and (a)(3), it will be presumed that the person receiving nonlegal services believes the services to be the subject of a client-lawyer relationship unless the lawyer or law firm has advised the person receiving the services in writing that the services are not legal services and that the protection of a client-lawyer relationship does not exist with respect to the nonlegal services, or if the interest of the lawyer or law firm in the entity providing nonlegal services is de minimis.

(b) Notwithstanding the provisions of paragraph (a), a lawyer or law firm that is an owner, controlling party, agent, or is otherwise affiliated with an entity that the lawyer or law firm knows is providing nonlegal services to a person shall not permit any nonlawyer providing such services or affiliated with that entity to direct or regulate the professional judgment of the lawyer or law firm in rendering legal services to any person, or to cause the lawyer or law firm to compromise its duty under Rule 1.6(a) and (c) with respect to the confidential information of a client receiving legal services.

(c) For purposes of this Rule, "nonlegal services" shall mean those services that lawyers may lawfully provide and that are not prohibited as an unauthorized practice of law when provided by a nonlawyer.

RULE 5.8.

Contractual Relationship Between Lawyers and Nonlegal Professionals

(a) The practice of law has an essential tradition of complete independence and uncompromised loyalty to those it serves. Recognizing this tradition, clients of lawyers practicing in New York State are guaranteed "independent professional judgment and undivided loyalty uncompromised by conflicts of interest." Indeed, these guarantees represent the very foundation of the profession and allow and foster its continued role as a protector of the system of law. Therefore, a lawyer must remain completely responsible for his or her own independent professional judgment, maintain the confidences and secrets of clients, preserve funds of clients and third parties in his or her control, and otherwise comply with the legal and ethical principles governing lawyers in New York State.

Multi-disciplinary practice between lawyers and nonlawyers is incompatible with the core values of the legal profession and therefore, a strict division between services provided by lawyers and those provided by nonlawyers is essential to protect those values. However, a lawyer or law firm may enter into and maintain a contractual relationship with a nonlegal professional or nonlegal professional service firm for the purpose of offering to the public, on a systematic and continuing basis, legal services performed by the lawyer or law firm as well as other nonlegal professional services, notwithstanding the provisions of Rule 1.7(a), provided that:

(1) the profession of the nonlegal professional or nonlegal professional service firm is included in a list jointly established and maintained by the Appellate Divisions pursuant to Section 1205.3 of the Joint Appellate Division Rules;

(2) the lawyer or law firm neither grants to the nonlegal professional or nonlegal professional service firm, nor permits such person or firm to obtain, hold or exercise, directly or indirectly, any ownership or investment interest in, or managerial or supervisory right, power or position in connection with the practice of law by the lawyer or law firm, nor, as provided in Rule 7.2(a)(1), shares legal fees with a nonlawyer or receives or gives any monetary or other tangible benefit for giving or receiving a referral; and

(3) the fact that the contractual relationship exists is disclosed by the lawyer or law firm to any client of the lawyer or law firm before the client is referred to the nonlegal professional service firm, or to any client of the nonlegal professional service firm before that client receives legal services from the lawyer or law firm; and the client has given informed written consent and has been provided with a copy of the "Statement of Client's Rights In Cooperative Business Arrangements" pursuant to section 1205.4 of the Joint Appellate Divisions Rules.

(b) For purposes of paragraph (a):

(1) each profession on the list maintained pursuant to a Joint Rule of the Appellate Divisions shall have been designated sua sponte, or approved by the Appellate Divisions upon application of a member of a nonlegal profession or nonlegal professional service firm, upon a determination that the profession is composed of individuals who, with respect to their profession:

(i) have been awarded a bachelor's degree or its equivalent from an accredited college or university, or have attained an equivalent combination of educational credit from such a college or university and work experience;

(ii) are licensed to practice the profession by an agency of the State of New York or the United States Government; and

(iii) are required under penalty of suspension or revocation of license to adhere to a code of ethical conduct that is reasonably comparable to that of the legal profession;

(2) the term "ownership or investment interest" shall mean any such interest in any form of debt or equity, and shall include any interest commonly considered to be an interest accruing to or enjoyed by an owner or investor.

(c) This Rule shall not apply to relationships consisting solely of non-exclusive reciprocal referral agreements or understandings between a lawyer or law firm and a nonlegal professional or nonlegal professional service firm.

RULE 6.1.

Voluntary Pro Bono Service

Lawyers are strongly encouraged to provide pro bono legal services to benefit poor persons.

(a) Every lawyer should aspire to:

(1) provide at least 50 hours of pro bono legal services each year to poor persons; and

(2) contribute financially to organizations that provide legal services to poor persons. Lawyers in private practice or employed by a for-profit entity should aspire to contribute annually in an amount at least equivalent to (i) the amount typically billed by the lawyer (or the firm with which the lawyer is associated) for one hour of time; or (ii) if the lawyer's work is performed on a contingency basis, the amount typically billed by lawyers in the community for one hour of time; or (iii) the amount typically paid by the organization employing the lawyer for one hour of the lawyer's time; or (iv) if the lawyer is underemployed, an amount not to exceed one-tenth of one percent of the lawyer's income.

(b) Pro bono legal services that meet this goal are:

(1) professional services rendered in civil matters, and in those criminal matters for which the government is not obliged to provide funds for legal representation, to persons who are financially unable to compensate counsel;

(2) activities related to improving the administration of justice by simplifying the legal process for, or increasing the availability and quality of legal services to, poor persons; and

(3) professional services to charitable, religious, civic and educational organizations in matters designed predominantly to address the needs of poor persons.

(c) Appropriate organizations for financial contributions are:

(1) organizations primarily engaged in the provision of legal services to the poor; and

(2) organizations substantially engaged in the provision of legal services to the poor, provided that the donated funds are to be used for the provision of such legal services.

(d) This Rule is not intended to be enforced through the disciplinary process, and the failure to fulfill the aspirational goals contained herein should be without legal consequence.

RULE 6.2.

[Reserved]

RULE 6.3.

Membership in a Legal Services Organization

A lawyer may serve as a director, officer or member of a not-for-profit legal services organization, apart from the law firm in which the lawyer practices, notwithstanding that the organization serves persons having interests that differ from those of a client of the lawyer or the lawyer's firm. The lawyer shall not knowingly participate in a decision or action of the organization:

(a) if participating in the decision or action would be incompatible with the lawyer's obligations to a client under Rules 1.7 through 1.13; or

(b) where the decision or action could have a material adverse effect on the representation of a client of the organization whose interests differ from those of a client of the lawyer or the lawyer's firm.

RULE 6.4.

Law Reform Activities Affecting Client Interests

A lawyer may serve as a director, officer or member of an organization involved in reform of the law or its administration, notwithstanding that the reform

may affect the interests of a client of the lawyer. When the lawyer knows that the interests of a client may be materially benefitted by a decision in which the lawyer actively participates, the lawyer shall disclose that fact to the organization, but need not identify the client. In determining the nature and scope of participation in such activities, a lawyer should be mindful of obligations to clients under other Rules, particularly Rule 1.7.

RULE 6.5.

Participation in Limited Pro Bono Legal Service Programs

(a) A lawyer who, under the auspices of a program sponsored by a court, government agency, bar association or not-for-profit legal services organization, provides short-term limited legal services to a client without expectation by either the lawyer or the client that the lawyer will provide continuing representation in the matter:

(1) shall comply with Rules 1.7, 1.8 and 1.9, concerning restrictions on representations where there are or may be conflicts of interest as that term is defined in these Rules, only if the lawyer has actual knowledge at the time of commencement of representation that the representation of the client involves a conflict of interest; and

(2) shall comply with Rule 1.10 only if the lawyer has actual knowledge at the time of commencement of representation that another lawyer associated with the lawyer in a law firm is affected by Rules 1.7, 1.8 and 1.9.

(b) Except as provided in paragraph (a)(2), Rule 1.7 and Rule 1.9 are inapplicable to a representation governed by this Rule.

(c) Short-term limited legal services are services providing legal advice or representation free of charge as part of a program described in paragraph (a) with no expectation that the assistance will continue beyond what is necessary to complete an initial consultation, representation or court appearance.

(d) The lawyer providing short-term limited legal services must secure the client's informed consent to the limited scope of the representation, and such representation shall be subject to the provisions of Rule 1.6.

(e) This Rule shall not apply where the court before which the matter is pending determines that a conflict of interest exists or, if during the course of the representation, the lawyer providing the services becomes aware of the existence of a conflict of interest precluding continued representation.

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.

(b) Subject to the provisions of paragraph (a), an advertisement may include information as to:

(1) legal and nonlegal education, degrees and other scholastic distinctions, dates of admission to any bar; areas of the law in which the lawyer or law firm practices, as authorized by these Rules; public offices and teaching positions held; publications of law related matters authored by the lawyer; memberships in bar associations or other professional societies or organizations, including offices and committee assignments therein; foreign language fluency; and bona fide professional ratings;

(2) names of clients regularly represented, provided that the client has given prior written consent;

(3) bank references; credit arrangements accepted; prepaid or group legal services programs in which the lawyer or law firm participates; nonlegal services provided by the lawyer or law firm or by an entity owned and controlled by the lawyer or law firm; the existence of contractual relationships between the lawyer or law firm and a nonlegal professional or nonlegal professional service firm, to the extent permitted by Rule 5.8, and the nature and extent of services available through those contractual relationships; and

(4) legal fees for initial consultation; contingent fee rates in civil matters when accompanied by a statement disclosing the information required by paragraph (p);

range of fees for legal and nonlegal services, provided that there be available to the public free of charge a written statement clearly describing the scope of each advertised service; hourly rates; and fixed fees for specified legal and nonlegal services.

(c) An advertisement shall not:

(1) include a paid endorsement of, or testimonial about, a lawyer or law firm without disclosing that the person is being compensated therefor;

(2) include the portrayal of a fictitious law firm, the use of a fictitious name to refer to lawyers not associated together in a law firm, or otherwise imply that lawyers are associated in a law firm if that is not the case;

(3) use actors to portray a judge, the lawyer, members of the law firm, or clients, or utilize depictions of fictionalized events or scenes, without disclosure of same; or

(4) be made to resemble legal documents.

(d) An advertisement that complies with subdivision (e) of this section may contain the following:

(1) statements that are reasonably likely to create an expectation about results the lawyer can achieve;

(2) statements that compare the lawyer's services with the services of other lawyers;

(3) testimonials or endorsements of clients, and of former clients; or

(4) statements describing or characterizing the quality of the lawyer's or law firm's services.

(e) It is permissible to provide the information set forth in subdivision(d) of this section provided:

(1) its dissemination does not violate subdivision(a)of this section;

(2) it can be factually supported by the lawyer or law firm as of the date on which the advertisement is published or disseminated;

(3) it is accompanied by the following disclaimer: "Prior results do not guarantee a similar outcome"; and

(4) in the case of a testimonial or endorsement from a client with respect to a matter still pending, the client gives informed consent confirmed in writing.

(f) Every advertisement other than those appearing in a radio, television or billboard advertisement, in a directory, newspaper, magazine or other periodical (and any web sites related thereto), or made in person pursuant to Rule 7.3(a)(1), shall be labeled "Attorney Advertising" on the first page, or on the home page in the case of a web site. If the communication is in the form of a self-mailing brochure or postcard, the words "Attorney Advertising" shall appear therein. In the case of electronic mail, the subject line shall contain the notation "ATTORNEY ADVERTISING."

(g) A lawyer or law firm shall not utilize meta tags or other hidden computer codes that, if displayed, would violate these Rules.

(h) All advertisements shall include the name, principal law office address and telephone number of the lawyer or law firm whose services are being offered.

(i) Any words or statements required by this Rule to appear in an advertisement must be clearly legible and capable of being read by the average person, if written, and intelligible if spoken aloud. In the case of a web site, the required words or statements shall appear on the home page.

(j) A lawyer or law firm advertising any fixed fee for specified legal services shall, at the time of fee publication, have available to the public a written statement clearly describing the scope of each advertised service, which statement shall be available to the client at the time of retainer for any such service. Such legal services shall include all those services that are recognized as reasonable and necessary under local custom in the area of practice in the community where the services are performed.

(k) All advertisements shall be pre-approved by the lawyer or law firm, and a copy shall be retained for a period of not less than three years following its initial

dissemination. Any advertisement contained in a computer-accessed communication shall be retained for a period of not less than one year. A copy of the contents of any web site covered by this Rule shall be preserved upon the initial publication of the web site, any major web site redesign, or a meaningful and extensive content change, but in no event less frequently than once every 90 days.

(l) If a lawyer or law firm advertises a range of fees or an hourly rate for services, the lawyer or law firm shall not charge more than the fee advertised for such services. If a lawyer or law firm advertises a fixed fee for specified legal services, or performs services described in a fee schedule, the lawyer or law firm shall not charge more than the fixed fee for such stated legal service as set forth in the advertisement or fee schedule, unless the client agrees in writing that the services performed or to be performed were not legal services referred to or implied in the advertisement or in the fee schedule and, further, that a different fee arrangement shall apply to the transaction.

(m) Unless otherwise specified in the advertisement, if a lawyer publishes any fee information authorized under this Rule in a publication that is published more frequently than once per month, the lawyer shall be bound by any representation made therein for a period of not less than 30 days after such publication. If a lawyer publishes any fee information authorized under this Rule in a publication that is published once per month or less frequently, the lawyer shall be bound by any representation made therein until the publication of the succeeding issue. If a lawyer publishes any fee information authorized under this Rule in a publication that has no fixed date for publication of a succeeding issue, the lawyer shall be bound by any representation made therein for a reasonable period of time after publication, but in no event less than 90 days.

(n) Unless otherwise specified, if a lawyer broadcasts any fee information authorized under this Rule, the lawyer shall be bound by any representation made therein for a period of not less than 30 days after such broadcast.

(o) A lawyer shall not compensate or give any thing of value to representatives of the press, radio, television or other communication medium in anticipation of or in return for professional publicity in a news item.

(p) All advertisements that contain information about the fees charged by the lawyer or law firm, including those indicating that in the absence of a recovery no fee will be charged, shall comply with the provisions of Judiciary Law §488(3).

(q) A lawyer may accept employment that results from participation in activities designed to educate the public to recognize legal problems, to make intelligent selection of counsel or to utilize available legal services.

(r) Without affecting the right to accept employment, a lawyer may speak publicly or write for publication on legal topics so long as the lawyer does not undertake to give individual advice.

RULE 7.2.

Payment for Referrals

(a) A lawyer shall not compensate or give anything of value to a person or organization to recommend or obtain employment by a client, or as a reward for having made a recommendation resulting in employment by a client, except that:

(1) a lawyer or law firm may refer clients to a nonlegal professional or nonlegal professional service firm pursuant to a contractual relationship with such nonlegal professional or nonlegal professional service firm to provide legal and other professional services on a systematic and continuing basis as permitted by Rule 5.8, provided however that such referral shall not otherwise include any monetary or other tangible consideration or reward for such, or the sharing of legal fees; and

(2) a lawyer may pay the usual and reasonable fees or dues charged by a qualified legal assistance organization or referral fees to another lawyer as permitted by Rule 1.5(g).

(b) A lawyer or the lawyer's partner or associate or any other affiliated lawyer may be recommended, employed or paid by, or may cooperate with one of the following offices or organizations that promote the use of the lawyer's services or those of a partner or associate or any other affiliated lawyer, or request one of the following offices or organizations to recommend or promote the use of the lawyer's services or those of the lawyer's partner or associate, or any other affiliated lawyer as a private practitioner, if there is no interference with the exercise of independent professional judgment on behalf of the client:

(1) a legal aid office or public defender office:

(i) operated or sponsored by a duly accredited law school;

(ii) operated or sponsored by a bona fide, non-profit community organization;

(iii) operated or sponsored by a governmental agency; or

(iv) operated, sponsored, or approved by a bar association;

(2) a military legal assistance office;

(3) a lawyer referral service operated, sponsored or approved by a bar association or authorized by law or court rule; or

(4) any bona fide organization that recommends, furnishes or pays for legal services to its members or beneficiaries provided the following conditions are satisfied:

(i) Neither the lawyer, nor the lawyer's partner, nor associate, nor any other affiliated lawyer nor any nonlawyer, shall have initiated or promoted such organization for the primary purpose of providing financial or other benefit to such lawyer, partner, associate or affiliated lawyer;

(ii) Such organization is not operated for the purpose of procuring legal work or financial benefit for any lawyer as a private practitioner outside of the legal services program of the organization;

(iii) The member or beneficiary to whom the legal services are furnished, and not such organization, is recognized as the client of the lawyer in the matter;

(iv) The legal service plan of such organization provides appropriate relief for any member or beneficiary who asserts a claim that representation by counsel furnished, selected or approved by the organization for the particular matter involved would be unethical, improper or inadequate under

the circumstances of the matter involved; and the plan provides an appropriate procedure for seeking such relief;

(v) The lawyer does not know or have cause to know that such organization is in violation of applicable laws, rules of court or other legal requirements that govern its legal service operations; and

(vi) Such organization has filed with the appropriate disciplinary authority, to the extent required by such authority, at least annually a report with respect to its legal service plan, if any, showing its terms, its schedule of benefits, its subscription charges, agreements with counsel and financial results of its legal service activities or, if it has failed to do so, the lawyer does not know or have cause to know of such failure.

RULE 7.3.

Solicitation and Recommendation of Professional Employment

(a) A lawyer shall not engage in solicitation:

(1) by in-person or telephone contact, or by real-time or interactive computer-accessed communication unless the recipient is a close friend, relative, former client or existing client; or

(2) by any form of communication if:

(i) the communication or contact violates Rule 4.5, Rule 7.1(a), or paragraph (e) of this Rule;

(ii) the recipient has made known to the lawyer a desire not to be solicited by the lawyer;

(iii) the solicitation involves coercion, duress or harassment;

(iv) the lawyer knows or reasonably should know that the age or the physical, emotional or mental state of the recipient makes it unlikely that the recipient will be able to exercise reasonable judgment in retaining a lawyer; or

(v) the lawyer intends or expects, but does not disclose, that the legal services necessary to handle the matter competently will be performed primarily by another lawyer who is not affiliated with the soliciting lawyer as a partner, associate or of counsel.

(b) For purposes of this Rule, "solicitation" means any advertisement initiated by or on behalf of a lawyer or law firm that is directed to, or targeted at, a specific recipient or group of recipients, or their family members or legal representatives, the primary purpose of which is the retention of the lawyer or law firm, and a significant motive for which is pecuniary gain. It does not include a proposal or other writing prepared and delivered in response to a specific request.

(c) A solicitation directed to a recipient in this State shall be subject to the following provisions:

(1) A copy of the solicitation shall at the time of its dissemination be filed with the attorney disciplinary committee of the judicial district or judicial department wherein the lawyer or law firm maintains its principal office. Where no such office is maintained, the filing shall be made in the judicial department where the solicitation is targeted. A filing shall consist of:

(i) a copy of the solicitation;

(ii) a transcript of the audio portion of any radio or television solicitation; and

(iii) if the solicitation is in a language other than English, an accurate English-language translation.

(2) Such solicitation shall contain no reference to the fact of filing.

(3) If a solicitation is directed to a predetermined recipient, a list containing the names and addresses of all recipients shall be retained by the lawyer or law firm for a period of not less than three years following the last date of its dissemination.

(4) Solicitations filed pursuant to this subdivision shall be open to public inspection.

(5) The provisions of this paragraph shall not apply to:

(i) a solicitation directed or disseminated to a close friend, relative, or former or existing client;

(ii) a web site maintained by the lawyer or law firm, unless the web site is designed for and directed to or targeted at persons affected by an identifiable actual event or occurrence or by an identifiable prospective defendant; or

(iii) professional cards or other announcements the distribution of which is authorized by Rule 7.5(a).

(d) A written solicitation shall not be sent by a method that requires the recipient to travel to a location other than that at which the recipient ordinarily receives business or personal mail or that requires a signature on the part of the recipient.

(e) No solicitation relating to a specific incident involving potential claims for personal injury or wrongful death shall be disseminated before the 30th day after the date of the incident, unless a filing must be made within 30 days of the incident as a legal prerequisite to the particular claim, in which case no unsolicited communication shall be made before the 15th day after the date of the incident.

(f) Any solicitation made in writing or by computer-accessed communication and directed to a pre-determined recipient, if prompted by a specific occurrence involving or affecting a recipient, shall disclose how the lawyer obtained the identity of the recipient and learned of the recipient's potential legal need.

(g) If a retainer agreement is provided with any solicitation, the top of each page shall be marked "SAMPLE" in red ink in a type size equal to the largest type size used in the agreement and the words "DO NOT SIGN" shall appear on the client signature line.

(h) Any solicitation covered by this section shall include the name, principal law office address and telephone number of the lawyer or law firm whose services are being offered.

(i) The provisions of this Rule shall apply to a lawyer or members of a law firm not admitted to practice in this State who shall solicit retention by residents of this State.

RULE 7.4.

Identification of Practice and Specialty

(a) A lawyer or law firm may publicly identify one or more areas of law in which the lawyer or the law firm practices, or may state that the practice of the lawyer or law firm is limited to one or more areas of law, provided that the lawyer or law firm shall not state that the lawyer or law firm is a specialist or specializes in a particular field of law, except as provided in Rule 7.4(c).

(b) A lawyer admitted to engage in patent practice before the United States Patent and Trademark Office may use the designation "Patent Attorney" or a substantially similar designation.

(c) A lawyer may state that the lawyer has been recognized or certified as a specialist only as follows:

(1) A lawyer who is certified as a specialist in a particular area of law or law practice by a private organization approved for that purpose by the American Bar Association may state the fact of certification if, in conjunction therewith, the certifying organization is identified and the following statement is prominently made: "The [name of the private certifying organization] is not affiliated with any governmental authority."

(2) A lawyer who is certified as a specialist in a particular area of law or law practice by the authority having jurisdiction over specialization under the laws of another state or territory may state the fact of

certification if, in conjunction therewith, the certifying state or territory is identified and the following statement is prominently made: "Certification granted by the [identify state or territory] is not recognized by any governmental authority within the State of New York."

(3) A statement is prominently made if:

(i) when written, it is clearly legible and capable of being read by the average person, and is in a font size at least two font sizes larger than the largest text used to state the fact of certification; and

(ii) when spoken aloud, it is intelligible to the average person, and is at a cadence no faster, and a level of audibility no lower, than the cadence and level of audibility used to state the fact of certification.

RULE 7.5.

Professional Notices, Letterheads and Signs

(a) A lawyer or law firm may use internet web sites, professional cards, professional announcement cards, office signs, letterheads or similar professional notices or devices, provided the same do not violate any statute or court rule and are in accordance with Rule 7.1, including the following:

(1) a professional card of a lawyer identifying the lawyer by name and as a lawyer, and giving addresses, telephone numbers, the name of the law firm, and any information permitted under Rule 7.1(b) or Rule 7.4. A professional card of a law firm may also give the names of members and associates;

(2) a professional announcement card stating new or changed associations or addresses, change of firm name, or similar matters pertaining to the professional offices of a lawyer or law firm or any nonlegal business conducted by the lawyer or law

firm pursuant to Rule 5.7. It may state biographical data, the names of members of the firm and associates, and the names and dates of predecessor firms in a continuing line of succession. It may state the nature of the legal practice if permitted under Rule 7.4;

(3) a sign in or near the office and in the building directory identifying the law office and any nonlegal business conducted by the lawyer or law firm pursuant to Rule 5.7. The sign may state the nature of the legal practice if permitted under Rule 7.4; or

(4) a letterhead identifying the lawyer by name and as a lawyer, and giving addresses, telephone numbers, the name of the law firm, associates and any information permitted under Rule 7.1(b) or Rule 7.4. A letterhead of a law firm may also give the names of members and associates, and names and dates relating to deceased and retired members. A lawyer or law firm may be designated "Of Counsel" on a letterhead if there is a continuing relationship with a lawyer or law firm, other than as a partner or associate. A lawyer or law firm may be designated as "General Counsel" or by similar professional reference on stationery of a client if the lawyer or the firm devotes a substantial amount of professional time in the representation of that client. The letterhead of a law firm may give the names and dates of predecessor firms in a continuing line of succession.

(b) A lawyer in private practice shall not practice under a trade name, a name that is misleading as to the identity of the lawyer or lawyers practicing under such name, or a firm name containing names other than those of one or more of the lawyers in the firm, except that the name of a professional corporation shall contain "PC" or such symbols permitted by law, the name of a limited liability company or partnership shall contain "LLC," "LLP" or such symbols permitted by law and, if otherwise lawful, a firm may use as, or continue to include in its name the name or names of one or more deceased or retired members of the firm or of a predecessor firm in a continuing line of succession. Such terms as "legal clinic," "legal aid," "legal service office," "legal assistance office," "defender office" and the like may be used only by qualified legal assistance organizations, except that the term "legal clinic" may be used by any lawyer or law firm provided the name of a participating lawyer or firm is incorporated therein. A lawyer or law firm may not include the name of a

nonlawyer in its firm name, nor may a lawyer or law firm that has a contractual relationship with a nonlegal professional or nonlegal professional service firm pursuant to Rule 5.8 to provide legal and other professional services on a systematic and continuing basis include in its firm name the name of the nonlegal professional service firm or any individual nonlegal professional affiliated therewith. A lawyer who assumes a judicial, legislative or public executive or administrative post or office shall not permit the lawyer's name to remain in the name of a law firm or to be used in professional notices of the firm during any significant period in which the lawyer is not actively and regularly practicing law as a member of the firm and, during such period, other members of the firm shall not use the lawyer's name in the firm name or in professional notices of the firm.

(c) Lawyers shall not hold themselves out as having a partnership with one or more other lawyers unless they are in fact partners.

(d) A partnership shall not be formed or continued between or among lawyers licensed in different jurisdictions unless all enumerations of the members and associates of the firm on its letterhead and in other permissible listings make clear the jurisdictional limitations on those members and associates of the firm not licensed to practice in all listed jurisdictions; however, the same firm name may be used in each jurisdiction.

(e) A lawyer or law firm may utilize a domain name for an internet web site that does not include the name of the lawyer or law firm provided:

(1) all pages of the web site clearly and conspicuously include the actual name of the lawyer or law firm;

(2) the lawyer or law firm in no way attempts to engage in the practice of law using the domain name;

(3) the domain name does not imply an ability to obtain results in a matter; and

(4) the domain name does not otherwise violate these Rules.

(f) A lawyer or law firm may utilize a telephone number which contains a domain name, nickname, moniker or motto that does not otherwise violate these Rules.

RULE 8.1.

Candor in the Bar Admission Process

(a) A lawyer shall be subject to discipline if, in connection with the lawyer's own application for admission to the bar previously filed in this state or in any other jurisdiction, or in connection with the application of another person for admission to the bar, the lawyer knowingly:

(1) has made or failed to correct a false statement of material fact; or

(2) has failed to disclose a material fact requested in connection with a lawful demand for information from an admissions authority.

RULE 8.2.

Judicial Officers and Candidates

(a) A lawyer shall not knowingly make a false statement of fact concerning the qualifications, conduct or integrity of a judge or other adjudicatory officer or of a candidate for election or appointment to judicial office.

(b) A lawyer who is a candidate for judicial office shall comply with the applicable provisions of Part 100 of the Rules of the Chief Administrator of the Courts.

RULE 8.3.

Reporting Professional Misconduct

(a) A lawyer who knows that another lawyer has committed a violation of the Rules of Professional Conduct that raises a substantial question as to that lawyer's honesty, trustworthiness or fitness as a lawyer shall report such knowledge to a tribunal or other authority empowered to investigate or act upon such violation.

(b) A lawyer who possesses knowledge or evidence concerning another lawyer or a judge shall not fail to respond to a lawful demand for information from a tribunal or other authority empowered to investigate or act upon such conduct.

(c) This Rule does not require disclosure of:

(1) information otherwise protected by Rule 1.6; or

(2) information gained by a lawyer or judge while participating in a bona fide lawyer assistance program.

RULE 8.4.

Misconduct

A lawyer or law firm shall not:

(a) violate or attempt to violate the Rules of Professional Conduct, knowingly assist or induce another to do so, or do so through the acts of another;

(b) engage in illegal conduct that adversely reflects on the lawyer's honesty, trustworthiness or fitness as a lawyer;

(c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;

(d) engage in conduct that is prejudicial to the administration of justice;

(e) state or imply an ability:

(1) to influence improperly or upon irrelevant grounds any tribunal, legislative body or public official; or

(2) to achieve results using means that violate these Rules or other law;

(f) knowingly assist a judge or judicial officer in conduct that is a violation of applicable rules of judicial conduct or other law;

(g) unlawfully discriminate in the practice of law, including in hiring, promoting or otherwise determining conditions of employment on the basis of age, race, creed, color, national origin, sex, disability, marital status or sexual orientation. Where there is a tribunal with jurisdiction to hear a complaint, if timely brought, other than a Departmental Disciplinary Committee, a complaint based on unlawful discrimination shall be brought before such tribunal in the first instance. A certified

copy of a determination by such a tribunal, which has become final and enforceable and as to which the right to judicial or appellate review has been exhausted, finding that the lawyer has engaged in an unlawful discriminatory practice shall constitute prima facie evidence of professional misconduct in a disciplinary proceeding; or

(h) engage in any other conduct that adversely reflects on the lawyer's fitness as a lawyer.

RULE 8.5.

Disciplinary Authority and Choice of Law

(a) A lawyer admitted to practice in this state is subject to the disciplinary authority of this state, regardless of where the lawyer's conduct occurs. A lawyer may be subject to the disciplinary authority of both this state and another jurisdiction where the lawyer is admitted for the same conduct.

(b) In any exercise of the disciplinary authority of this state, the rules of professional conduct to be applied shall be as follows:

(1) For conduct in connection with a proceeding in a court before which a lawyer has been admitted to practice (either generally or for purposes of that proceeding), the rules to be applied shall be the rules of the jurisdiction in which the court sits, unless the rules of the court provide otherwise; and

(2) For any other conduct:

(i) If the lawyer is licensed to practice only in this state, the rules to be applied shall be the rules of this state, and

(ii) If the lawyer is licensed to practice in this state and another jurisdiction, the rules to be applied shall be the rules of the admitting jurisdiction in which the lawyer principally practices; provided, however, that if particular conduct clearly has its predominant effect in another jurisdiction in which the lawyer is licensed to practice,

the rules of that jurisdiction shall be applied to that conduct.

Tinker, Tailor, Lawyer, P.I.: Are Your Workplace Investigations Complying with the Law?

June 2, 2015 • NYLER Archive

By Ronald C. Minkoff, Lindsay Harris, and Andrew Jacobs

The recent high-profile trial in *Ellen Pao vs. Kleiner Perkins,* No. CGC-12-520719 (S.F. Cty. Super. Ct. filed 5/10/2012), in which Pao unsuccessfully sued her employer, venture capital firm Kleiner Perkins, for gender discrimination and other claims, highlights the increasingly important role of attorneys who are retained by organizations to conduct impartial investigations of alleged workplace discrimination, retaliation, and harassment. Though not as widely covered by the mainstream media as other aspects of the case, the trial included crucial testimony from an attorney whom Kleiner Perkins had retained to independently investigate Ms. Pao's complaints, as well as from opposing experts who testified with respect to the adequacy of that attorney's investigation.

Many lawyers who perform such workplace investigations — in Silicon Valley and beyond —face confusion about their proper role and the ethical duties that govern them. In conducting such investigations, are they acting as attorneys? If so, how can they be impartial? And if not, in what capacity do they act? Moreover, increasingly, these questions are finding their way into court cases and judicial and administrative decisions. For example, at trial, the judge in *Pao* asked the employer's expert whether the employer's attorney investigator possessed authority under state law, absent a private investigator's license, to conduct the type of workplace investigation he did.

Faced with such riddles, lawyers who conduct workplace investigations have taken different tacks. While some conduct investigations in their capacity "as attorneys," many do not. Of those who do not, some structure their investigative engagements ambiguously, leaving it unclear whether they are acting as attorneys or not, while still others explicitly state in their engagement agreements that they are *not* acting as attorneys. Although not licensed private investigators, these attorneys insist they are not performing legal services in connection with the investigation. They contend that eschewing an attorney-client relationship and the responsibility to advocate for a particular client is the only way to ensure their investigation is truly impartial. They further contend that, since they are not acting as attorneys, the full range of attorney ethics rules do not apply to their investigative work.

In this article, we will show that this approach, when applied to workplace investigations in New York, violates New York's statutory scheme, which allows attorneys to conduct workplace investigations without a private investigator's license only if they are acting "in the regular practice of their profession." Moreover, this approach misperceives the flexibility built into New York's Rules of Professional Conduct (RPCs), particularly RPCs 1.2(c) and 2.3, which allow lawyers to limit their roles to purely impartial investigative functions. Finally, it ignores that while the RPCs do place strictures on what attorneys can do in investigations, they also provide advantages that non-attorney investigators do not have — most notably, the attorney-client privilege and work product protection.

New York Private Investigator Licensure Requirement & Attorney Exemption

New York, like most other states, requires private investigators to be licensed. Under New York General Business Law §70(2) (N.Y. GBL) (McKinney 2011), no person or entity "shall engage in the business of private investigator…without having first obtained from the department of state a license so to do." N.Y. GBL §83, however, specifically exempts practicing attorneys from the licensure requirement, providing that "[nothing] contained in this article shall be construed to affect in any way attorneys or counselors at law in the regular practice of their profession" Similar exemptions exist in many other states.

Attorney Investigations Fall Within Scope of 'Private Investigation'

N.Y. GBL §83 implicitly recognizes that lawyers' activities often encompass "private investigation," as defined by New York law. This is particularly true of attorneys who conduct workplace investigations, which typically include gathering and review of documents, interviews of witnesses, and summarizing the available facts to determine if improper acts or omissions occurred. N.Y. GBL §71(1) defines "private investigator" broadly enough to encompass these activities, as it includes persons who investigate "the identity, habits, [and] conduct … of any person, group of persons, … firm or corporation," "the credibility of witnesses or other persons," and "the conduct, honesty, efficiency, loyalty or activities of employees, agents, contractors, and sub-contractors." The definition also includes "the securing of evidence to be used before any authorized investigating committee, board of award, board of arbitration, or in the trial of civil or criminal cases." *See Id*. In short, New York's definition of "private investigation" encompasses the sort of factual inquiry often performed by attorneys.

This conclusion is confirmed by Megibow 397-DOS-13 (2011), a recent New York Department of State decision granting a former attorney's application for a private investigator's license. Under N.Y. GBL §72 there are certain experience requirements which private investigator applicants must meet in order to obtain a license:

Every such applicant for a license as private investigator shall establish to the satisfaction of the secretary of state…[that s/he] ***has been regularly employed, for a period of not less than three years***, undertaking such investigations as those described as performed by a private investigator in N.Y. Gen. Bus. Law §71(1) (McKinney 2011), as a sheriff, police officer in a city or county police department, or the division of state police, investigator in an agency of the state, county, or United States government, or employee of a licensed private investigator, ***or has had an equivalent position and experience***." (Emphasis added.)

A regulation, 19 NYCRR §172.1, sets forth what constitutes "an equivalent position and experience" for purpose of N.Y. GBL §72 listing investigations largely corresponding to those found in N.Y. GBL §71(1), and requiring that "such investigations were conducted on a full-time basis in a position the primary duties of which were to conduct investigations."

In 2011, Steven Megibow, an attorney licensed to practice in New York, applied for a private investigator's license on the basis of his experience working in a non-legal capacity at two private investigation firms. His application was denied because he had only 30 months of creditable investigation experience at those firms, rather than the required 36 months. 507-DOS-11 at 1. Megibow argued that he should also be credited for one year of "full-time investigations experience" from his previous employment as an associate at the law firm Kramer Levin Naftalis & Frankel LLP (Kramer Levin). At a hearing, testimony was presented that Kramer Levin had been retained by a publicly traded company's Audit Committee to conduct an

internal investigation into potential financial and accounting misfeasance at the company. Megibow worked full-time as a junior associate on the matter, with duties including "reviewing and analyzing documents acquired from the subject; evaluating evidence; preparing investigative outlines and issues to be discussed; interviews of witnesses; identifying witnesses to be interviewed; [and] conducting interviews." *Id.* at 7. Kramer Levin's role was purely investigatory; the company had separate litigation and general corporate counsel. *Id.* at 8. Relying on these facts, the Administrative Law Judge held that Megibow's time at Kramer Levin constituted "creditable experience to be granted a license as a private investigator," such that his six-month experience deficiency was cured. 397-DOS-13 at 2.

The definition of "private investigator" in N.Y. GBL §71(1) and *Megibow* thus demonstrate the overlap between the work of an attorney and work that constitutes "private investigation" under New York law. N.Y. GBL §83 thus serves the important function of exempting "attorneys or counselors at law in the regular practice of their profession" from the need to obtain a separate private investigator's license.

'Factual' Investigations By Attorneys Constitute 'Regular Practice of Their Profession'

Still, the question remains whether workplace investigations by attorneys constitute "the regular practice of the [legal] profession" under N.Y. GBL §83. While no New York court has squarely addressed that question, the Court of Appeals has held that materials generated by a law firm during its conduct of an internal investigation are protected by the attorney-client privilege. In *Spectrum Systems Intern. Corp. v. Chemical Bank,* 78 N.Y.2d 371 (1991), the Court held that the privilege applied to the report of plaintiff's outside counsel of an internal investigation into possible fraud involving the defendant. The Court acknowledged the "conceded investigative function" of outside counsel and that their final report "did not focus on any imminent litigation," "reflected no legal research," and "was inconclusive, looking toward further discussion." *See id.* at 378–81. Nevertheless, it held that the material was "primarily and predominantly of a legal character" because it "relate[d] and integrate[d] the facts with the law firm's assessment of the client's legal position." *Id.* at 380.

Although *Spectrum Systems* involved application of the attorney-client privilege rather than N.Y. GBL §83, it suggests that investigative work by attorney's, even if preliminary and mainly factual, constitutes the "regular practice of their profession" under N.Y. GBL §83, regardless of whether the assessment involves legal research or comes to an ultimate legal conclusion. This should come as welcome news for workplace investigators in New York, who typically provide factual findings, or findings on whether the employer's policy was violated, but do not typically render "legal advice" as that term is commonly understood, for example, advising the employer on legal steps to take based on the investigation. (That function is usually performed by the organization's regular outside or in-house counsel.)

Under the analysis in *Spectrum Systems,* 78 N.Y.2d at 378–79, as well as that of a growing number of federal courts, the sort of factual investigations commonly performed by these attorneys would fall within the protection of N.Y. GBL §83. *See e.g., Gruss v. Zwirn,* 276 F.R.D. 115, 122–27 (S.D.N.Y. 2011), "[i]nterviews of a corporation's employees by its attorneys as part of an internal investigation into wrongdoing and potentially illegal conduct have been repeatedly found to be protected by the attorney-client privilege" (applying New York law); *revd. on other grounds*, 2013 WL 3481350 (S.D.N.Y. 7/10/2013); *see also, Sandra T.E. v. S. Berwyn Sch. Dist. 100* [600 F.3d 612, 620 (7th Cir. 2010)], "[W]hen an attorney conducts a factual investigation in connection with the provision of legal services…communications in the course of the investigation are fully protected by the attorney-client privilege."

This result is consistent not only with the New York law of attorney-client privilege, but with the general principle that "the practice of law relates to the rendition of services to others that call for the professional judgment of a lawyer." Ethical Consideration 3–5 to the former N.Y. Code of Professional Responsibility; *see also,* ABA Task Force on the Model Definition of the Practice of Law (still good authority given that current RPC 5.5 is identical to former DR 3-101, governing the unauthorized practice of law); Proposed Model Definition, Sept. 18, 2002, "The 'practice of law' is the application of legal principles and judgment with regard to the circumstances or objectives of a person that require the knowledge and skill of a person trained in the law." As *Spectrum Systems,* 78 N.Y.2d at 380, and the other cases cited show, a factual investigation often does involve "the professional judgment of a lawyer," even if no ultimate legal conclusion is reached.

Being an Attorney Alone Is Insufficient to Guarantee Protection of GBL §83

While N.Y. GBL §83 protects attorneys acting "in the regular practice of their profession" from private investigator license requirements, an individual's mere status as an attorney will not provide an exemption from those requirements. Megibow 397-DOS-13 (2011), is again instructive on this point. As noted above, Megibow's application was initially denied because his creditable experience at investigative firms did not total three years, in part because one of the investigative firms at which he worked did not have a private investigator's license for six of the months for which Megibow sought credit. *See* 507-DOS-11 at 3.

On appeal, Megibow argued that because attorneys are exempt from licensure requirements, *all* of his non-legal work at the investigative firm was creditable as qualifying experience, whether the firm had a private investigator license or not. This argument failed: Because the investigative firm was neither "licensed as a private investigator" nor "authorized to render professional legal services," its business violated N.Y. GBL §70(2), and Megibow's investigative work at the firm during that period was not creditable. *See* 39-DOS-APP-12 at 5. This aspect of *Megibow* makes clear that unless attorneys are acting "in the regular practice of their profession" (or are employees of a licensed private investigator), they are not exempt from N.Y. GBL §70(2) requirement of obtaining a private investigator's license. In sum, in order to be deemed as acting "in the regular practice of their profession," attorney investigators must possess an active law license (including authority to practice law in New York); must conduct their investigations within the context of an attorney-client relationship; and remain, in the conduct of the investigation, subject to the full panoply of legal ethical duties.

The short of it is that attorneys who perform workplace investigations while disavowing the existence of an attorney-client relationship are breaking the law. These attorneys place themselves in a double-bind: By presenting the services as non-legal, they are unlikely to be deemed as acting "in the regular practice of their profession," and thus, unless they possess a separate private investigator's license, are violating N.Y. GBL §70(2). At the same time, New York courts and disciplinary bodies are likely to view the services as nonetheless subject to the full panoply of legal ethics rules, because, as discussed further below, New York law generally presumes that services offered by an attorney — or even acts taken by an attorney in her non-legal capacity — are subject to the RPCs. This places the attorney between the proverbial rock and a hard place — especially if, under the misconception that the RPCs did not apply, he or she has failed to observe them in conducting the investigation. For example, the attorney may have failed to observe the so-called "no contact" rule [RPC 4.2] — a not uncommon error of attorney investigators who think they are not "acting as attorneys." Therefore, in attempting to conduct an investigation as a "non-legal" service, such an attorney may have unwittingly violated both New York's private investigator law, as well as the RPCs.

The potential consequences for this illegal conduct are severe. Under N.Y. GBL §70(4), a person who violates the private investigator licensing requirements is guilty of a Class B misdemeanor, punishable by up to three months in jail, a $500 fine, and possible additional financial penalties. N.Y. Penal Law §70.15 and §80.05. Moreover, the violator faces disciplinary consequences for committing a crime and/or misrepresenting his or her qualifications. *See* RPCs 8.4(b) and (c), an attorney shall not "engage in illegal conduct that adversely reflects on the lawyer's honesty, trustworthiness or fitness as a lawyer" or "engage in conduct involving dishonesty, fraud, deceit or misrepresentation." The violator also could face civil liability, or the loss of privileged status of his or her communications with the employer. An investigation that was not conducted under a proper license (i.e., under either a private investigator's or law license) also could be challenged in litigation on the grounds that the investigation was conducted unlawfully; this has actually happened in California. Complaint, *Jolly Tech., Inc. vs. Robert Half Intl., Inc.*, No. CIV529256, (San Mateo Super. Ct. 6/25/2014). Finally, out-of-state attorneys who conduct workplace investigations in New York but who are not authorized to practice law in New York could face discipline for the unauthorized practice of law, or see their investigations challenged on this ground in civil litigation.

An Attorney May Structure Relationship with Client to Ensure an Impartial Investigation

For all these reasons, unless they are prepared to apply for a private investigator's license under N.Y. GBL §72, investigative attorneys should embrace, rather than distance themselves from, the label "attorney." Doing so will not, as some attorneys fear, mean they cannot conduct an independent and impartial investigation. The RPCs allow investigative attorneys to structure their client-attorney relationships so that they can act independently.

Limited Scope Representation

In this regard, investigative attorneys may look to RPC 1.2(c). This provision, added to New York's ethics rules when the RPCs were adopted in 2009, allows attorneys to limit the scope of their representation under certain conditions:

"A lawyer may limit the scope of the representation if the limitation is reasonable under the circumstances, the client gives informed consent, and where necessary notice is provided to the tribunal and/or opposing counsel."

This allows the attorney, with the informed consent of the client, to adjust both the scope and objectives of the representation to suit the client's needs. "A limited representation may be appropriate because the client has limited objectives for the representation." RPC 1.2, Comm. 6. All that is required is that the limitation be reasonable, *i.e.,* so it does not interfere with the attorney's "duty to provide competent representation" *Id.* Comm. 7, and that the attorney obtain informed consent after disclosing "the reasonably foreseeable consequences of the limitation." *Id.* Comm. 6A.

Even assuming that the investigative attorney would otherwise be required to "favor" the employer-client in conducting an investigation — a proposition we consider dubious, but which finds some support, in RPC 1.1(c)(2) (prohibiting a lawyer from "prejudic[ing] or damag[ing] the client during the course of the representation") — compliance with RPC 1.2(c) solves the problem. If the client wants a truly independent

investigation, the attorney can provide it by obtaining the necessary informed consent. Once again, Megibow 397-DOS-13 (2011), provides a perfect example. There, Kramer Levin was asked to perform a purely investigative function, reporting on facts uncovered while the corporate client had other attorneys analyze those facts and advise the Board. This allowed Kramer Levin to be fully independent and impartial in its work, knowing the client's other lawyers would protect its interests. RPC 1.2(c) provides the vehicle for this kind of limitation.

Evaluation for Use by Third Persons

The RPCs provide an even more specific provision for investigative attorneys. RPC 2.3 addresses investigative reports and opinion letters, particularly when written to be shown to third parties, and is intended to address the concerns stemming from RPC 1.1(c)(2)s prohibition on intentionally "prejudice[ing] or damag[ing]" a client. *See Simon's N.Y. Rules of Prof. Conduct Annotated* at 817 (West 2014). It permits the investigative report to "provide an evaluation of a matter affecting the client for the use of someone other than the client if the lawyer reasonably believes that making the evaluation is compatible with other aspects of the lawyer's relationship with the client." RPC 2.3(a) allows the lawyer to reveal even confidential information if doing so "'advance[s] the best interests of the client' (if reasonable or customary) but does not grant implied authority to harm the client." *Simon's N.Y. Rules* at 818, citing RPC 1.6(a)(2). But RPC 2.3 goes even further: It allows the investigative attorney to reveal in the report information which is "likely to affect the client's interests materially and adversely" as long as the client gives "informed consent." [RPC 2.3(b).] Absent such authorization, "information relating to the evaluation is protected by Rule 1.6." RPC 2.3(c).

This Rule speaks directly to attorneys who, for example, conduct workplace investigations with the understanding that results might be disclosed to the EEOC, the SEC or the U.S. Attorney's office. It permits them to make disclosures to these agencies and other third parties about their client — even adverse disclosures — as long as the client gives "informed consent." *See* RPC 1.0(j), defining that phrase, and requiring attorney to "adequately explain[]" to the client the "material risks of the proposed course of conduct and reasonably available alternatives."

But implicit in all this is that an attorney, when conducting an investigation, may ferret out all information relevant to advise the client, even if that information proves unfavorable. Indeed, a lawyer has an obligation to "promptly inform the client of…any decision or circumstance" for which the client's informed consent is required [RPC 1.4(a)(1)(i)], and to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." RPC 1.4(b). Thus, the RPCs do not just allow an impartial and independent investigation: they demand it. What the client does with any adverse information uncovered is then between the client and its attorney, with the attorney obligated to obtain the client's "informed consent" before disclosing that information to a third party. RPCs 2.3(b) and (c).

Protections of Attorney-Client Relationship

It is true that in some instances, attorneys offering so-called "non-legal" services may take off their "attorney hat," and avoid the strictures of the RPCs. *See* RPC 5.7(c), defining "nonlegal services" as "those services that lawyers may lawfully provide and that are not prohibited as an unauthorized practice of law when provided by a nonlawyer." However, doing so is difficult: RPC 5.7, which addresses an attorney's responsibilities with respect to non-legal services, presumes that services offered by an attorney are

subject to the RPCs, unless the services are "distinct" from any legal services offered to the client, *and* the attorney provides an appropriate written disclaimer to the client. RPC 5.7(a)(4) disclaimer. The disclaimer must state that the services are not legal services and that the protections of the lawyer client relationship do not exist with respect to the non-legal services. RPC 5.7(a)(4).

But we should leave no doubt: For the reasons discussed above, providing an RPC 5.7(a)(4) disclaimer in the context of workplace investigations is not a viable option (except perhaps for an attorney working directly for a private investigation firm). And even if it were, there are other reasons why it is not a good idea. For one thing, it deprives the employer of two important protections — the attorney-client privilege and the work product protection. It is axiomatic that to invoke either of those protections, the employer must be dealing with an attorney in an attorney-client relationship. *See, e.g.,* RPC 1.6, Comm. 3 ("The attorney-client privilege and the work-product doctrine apply when compulsory process by a judicial or other governmental body seeks to compel a lawyer to testify or produce information *concerning a client.*") (emphasis added); N.Y. County Lawyers' Assn. Comm. on Prof. Ethics Formal Op. 717 (1996) (discussing if a lawyer/employee of an insurance company is not acting as an attorney, former DR 4-101, (the predecessor to RPC 1.6), does not apply); Weinstein, Korn & Miller, *New York Civil Practice* §3101.45 at 31–120 ("Work product protection seeks to maintain the sanctity of the attorney's legal work and thought while the privilege seeks to protect the client's freedom of revelation and right of privacy"); *but see e.g., U.S. v. Kovel,* 296 F.2d 918 (2d Cir. 1961) (discussing communications between client and others hired by the attorney whose presence is necessary for effective consultation between client and the attorney are still covered by the privilege, even if attorney not present).

To disclaim the attorney-client relationship is to disclaim these important protections, which could result in government investigators and others obtaining sensitive and confidential information to which they otherwise would not be privy. Nor, arguably, does the privilege merely serve the employer's interest. Rather, by creating a protected zone within which organizations can investigate potential misconduct, as well as by promoting candor between lawyer and client, the privilege is thought to "promote broader public interests in the observance of law and the administration of justice." *Upjohn Co. vs. United States*, 449 U.S. 383, 389 (1981).

Of course, the existence of an attorney-client relationship imposes additional obligations on the investigative attorneys. For example, attorneys have certain duties in communicating with third parties that non-lawyers do not possess, such as the duty already noted under RPC 4.2(a) not to communicate with persons known to be represented by counsel without their counsel's consent, the duty under RPC 1.13(a) to provide adequate warnings as to the lawyer's identity and role, and the duty under RPC 1.13(b) to make disclosures and "climb the ladder" if wrongdoing is uncovered. Nonetheless, attorneys who currently conduct workplace investigations "as attorneys" do not report that complying with these or other attorney ethics rules has impeded their ability to conduct fair and effective investigations.

And in some cases, courts have gone out of their way to protect lawyers conducting internal investigations for employers against claims that they developed a separate attorney-client relationship with the employees they interviewed. *See, e.g., U.S. v. Ruehle,* 583 F.3d 600 (9th Cir. 2009) (holding that a corporate officer had no reasonable expectation that interview with corporation's lawyer was confidential even though firm did not give "corporate Miranda" warning and firm had represented officer previously on personal matter); *U.S. v. Weissman,* 195 F.3d 96 (2d Cir. 1999) (discussing that there was no common interest privilege found at meeting between employee, employer and employer's lawyer because existence of common interest not made explicit at meeting); *Matter of Bevill, Bressler & Schulman Asset Mgmt. Co.,* 805 F.2d 120 (3d Cir. 1986) (imposing strict five-part test for determining that corporate employee is represented by corporation's lawyer).

In short, clarifying the attorney investigator's proper role as that of an attorney arguably enhances his or her ability to conduct fair, impartial and effective workplace investigations — because the rules of the road, including the ethical duties and standards that apply, are well-established and clear to all participants.

Conclusion

Under N.Y. GBL §83, only attorneys engaged "in the regular practice of their profession" are permitted to conduct workplace investigations without a private investigator's license. Just as important, the idea that investigative attorneys must eschew the attorney-client relationship in order to maintain their independence is a myth; under RPCs 1.2(c) and 2.3, investigative attorneys can craft limited scope engagements with their employer clients that afford them all the independence they need, even to the point of disclosing adverse information to third parties. Finally, the burdens an attorney-client relationship imposes on investigative attorneys are few, but the advantages, particularly from the attorney-client privilege and work product protection, are vast. Attorneys conducting work-place investigations should embrace their role as attorneys, not reject it. Doing so is better for them, better for their clients and better for the public.

Ronald C. Minkoff is the Head of the Professional Responsibility Group at Frankfurt Kurnit Klein & Selz, P.C. Andrew Jacobs is an associate at that firm. Lindsay Harris is the founding principal of West Coast Workplace Investigations, an Internal Investigations Law Firm in Berkeley, California, and serves on the Board of Directors of the Association of Workplace Investigators, a professional member association focused on promoting and enhancing the quality of impartial workplace investigations.

Get CLE Credit for this month's articles (June 2015).

« Understanding & Securing the LLP Shield in New York (Part 1) Recent N.Y. Ethics Opinions: July/August 2015 »

By Martin I. Kaminsky (Greenberg Traurig) and Maren J. Messing (Patterson Belknap Webb & Tyler)

Lawyers sometimes want to contact a person who is connected with an adverse party or formerly connected with an adverse party in a transaction or litigation. It may surprise you to learn that, while you generally cannot do that, you sometimes can. To avoid problems and complaints you need to understand the rules and the limits and spirit of the rules.

This article, which will be published in two parts, provides practical guidance on applicable rules and ethics opinions considering common situations that attorneys encounter. For the most part, it addresses only New York law; but reference in some instances will be made to differing ABA or state ethical rules and the law of other jurisdictions. Part I of the article explains the general "no contact" rule and the consequences of failure to adhere to it. Part II, to follow in another edition of **NYLER,** will explain the applicability *vel non* of the Rule to entities and their current or former employees and the nature of the discussions that may or may not be had.

What Are the Guiding Rules?

The starting point is Rule 4.2(a) of the New York Rules of Professional Conduct (NYRPC). It provides that "a lawyer shall not communicate about the subject of a representation with a party" who the lawyer "knows to be represented by another lawyer in the matter" unless the lawyer has the consent of the other lawyer or the contact is "authorized to do so by law." NYRPC Rule 4.2(a). The Rule is substantially similar to prior N.Y. Disciplinary Rule 7-104(A) NYSBA Comm. Prof. Eth., Op. 904 (2014).

The Rule applies to communications made in connection with both transactional and litigation matters. Indeed, the Rule may apply even before the matter occurs if the communication is made as to a potential matter and the lawyer knows that that the person he/she is seeking to speak to is represented in that matter by counsel. NYSBA Comm. Prof. Eth., Op. 735 (2001). *See, e.g., McHugh v. Fitzgerald,* 280 A.D.2d 771, 772 (NY App. Div. 3d Dept. 2001) ("commencement of the litigation is not the criteria for determining whether communication with an adverse party is in derogation of the cited rule"); *United States v. Jamail,* 707 F.2d 638, 646 (2d Cir. 1983) (the prohibition applies to criminal investigations prior the actual commencement of a proceeding). But, as discussed further below, bar opinions and case law sometimes differentiate between civil and criminal cases and give greater latitude to investigations of possible criminal conduct. NYSBA Comm. Prof. Eth., Op. 884 (2011). *See e.g.*, *Gidatex v. Campaniella Imports Ltd.,* 82 F. Supp. 2d 119, 123 (S.D.N.Y. 1999).

The Rule also applies to all parties in a matter, not only those who are adverse to your client. NYRPC Rule 4.2(a). In other words, when you know another party has counsel in the matter,

absent consent or legal right, you cannot communicate with that other party, regardless of the type of matter involved or the role of that party in the matter. *Id.*

The Rule does not prohibit communications about matters other than "the subject matter" of the transaction or litigation at issue. *Id.* But, a lawyer is well-advised to avoid such communications, particularly a conversation, lest it later raise questions in the mind of a jury or judge as to what was really said. Further, as a practical matter, there would appear to be little need or reason for such a communication on other matters at that time.

Does It Matter That Rule Speaks of 'Parties' Rather Than 'Persons'?

Significantly, the New York rule speaks in terms of a "party." In contrast, the ABA Model Rule, and that of several other states (*e.g.*, New Jersey, Texas, District of Columbia, and others), provides that such communications may not be had with any "person" who is represented by counsel in the matter. Thus, on its face, the New York Rule sets forth a narrower prohibition than that of others. *Id.* As will be explained in Part II of this article, particularly when dealing with an organization or a witness, the New York Rule affords greater latitude than many other jurisdictions. *See infra* Part II. Differently, the other subpart of New York Rule 4.2 (also to be discussed in Part II) speaks in terms of "persons" not merely "parties." *Id.* In this regard, Professor Roy Simon explains that the choice of the word "party" was a purposeful and deliberate change in 2009 from the text originally suggested by those recommending that New York adopt the ABA Model Rules to replace the former Disciplinary Rules and Ethical Considerations. *Simon's Rules of Professional Conduct*, 1187 (2014). Prosecutors had expressed concern that a broad no-contact rule covering non-parties would or could impair their ability to prepare criminal cases. NYSBA Comm. Prof. Eth., Op. 884 (2011).

This distinction can be important. For example, ABA Formal Opinion 07-445 (2007) concluded that, in a civil context, putative class members are not "parties" for purposes of the no-contact rule, and do not become parties until a class including them has been certified. But one must be careful relying on this interpretation; some courts have determined the opposite. *See e.g.*, *Dondore v. NGK Metals Corp.,* 152 F. Supp. 2d 662, 665 (E.D. Pa. 2001); *see also, Gulf Oil Co. v. Bernard,* 452 U.S. 89, 104 (1981).

Apart from situations where special policy reasons may apply, New York courts and others have not always applied the distinction literally, particularly in non-criminal matters. For example, in NYSBA Opinion 607 (1990), the Committee gave the word "party" an "expansive definition" to apply to a potential party in a potential matter. Similarly, in NYSBA Opinion 735 (2001), the Committee concluded that the Rule could apply to an accountant represented by counsel even though not itself a party. Relying on the spirit of the Rule, the Opinion concluded that, regardless of its wording, the Rule applies to "represented witnesses, potential witnesses and others with an interest or right at stake, although they are not nominal parties" in the matter. *Id.*

As explained in NYSBA Opinion 884 (2011), which traces the history of the language, Rule 4.2 is given a more restrictive interpretation in criminal matters than civil matters. The Committee concluded that counsel for a defendant in a robbery case could contact a non-party witness even

though he knew the witness had an attorney, distinguishing the issue there from contacting a witness in civil cases. *Id.* In addition, the Committee reasoned that such a witness can always insist on including his/her counsel in the communication, even if the witness is contacted directly. *Id.* Further, the Committee explained, counsel for the witness can advise his/her client not to speak to the inquiring lawyer without concern that to do so would violate the prohibitions in New York Rules 3.4(a)(1) and (2) and 8.4(b) and (d) against suppressing evidence and assisting wrongdoing. *Id.*

Does It Matter If You Don't Make Contact Yourself?

Rule 4.2 is clear that it covers not only communications directly between a lawyer and another represented party, but also prohibits a lawyer from "caus[ing] another to communicate" in his/her place. NYRPC Rule 4.2(a). That part of the rule is meant to prevent the use of third persons, including investigators, to ferret out information from represented parties on a lawyer's behalf; and it is given a broad interpretation. *Id.* For example, in *United States v. Hammad,* 858 F.2d 834, 836 (2d Cir. 1988), *cert. denied*, 498 U.S. 871 (1989), the Rule was found applicable to a supplier of the target of a Medicaid fraud investigation whom the prosecutor used to obtain an admission of wrongdoing from the target. The court concluded that the supplier was the "alter ego" of the prosecutor in that instance. *Id.*

Similar "alter ego" analysis would lead to the same conclusion as to other persons in a lawyer's firm, whether attorneys or other employees such as paralegals or staff persons. *See,* NYC Bar Assn. Comm. Prof. Jud. Eth., Formal Op. 1995-11 (1995) (lawyers are responsible for the acts of non-lawyers under their supervision). *See also,* former N.Y. DR 1-104(A); *In re* Bonanno, 617 NYS2d 584, 584 (3d Dept. 1994) (censure of attorney for insufficient supervision of legal assistant). This analysis is consistent with the prohibition in New York Rule 8.4(a) that "[a] lawyer or law firm shall not violate" any of the Rules or "do so through the acts of another." NYRPC Rule 4.2(a). New York Rule 5.3 also imposes a duty on lawyers to supervise those working for them, including non-lawyers. Thus, in simplest terms, lawyers are advised to honor the spirt of the Rule, and not look for loopholes or try to "lawyer" around it.

There are, however, some exceptions to the Rule. These exceptions are discussed below and will be further amplified in Part II.

What If the Person's Lawyer Doesn't Respond?

The Rule creates an exception if a party's counsel consents to a lawyer directly contacting the party. On the other hand, what does a lawyer do if counsel for a party simply ignores her request or otherwise fails to respond to it?

Early ethics opinions tied the lawyer's hands in this situation, concluding that contact is not possible in that instance unless there has been an affirmative indication of a termination of the attorney-client relationship between the silent lawyer and the person you want to contact. *See*

e.g., N.Y. Cty. Law. Assn., Op. 625 (1974); NYC Bar Assn. Comm. Prof. Jud. Eth., Informal Op. 827 (1965). More recently, NYSBA Opinion 663 (1994) took a more practical view, concluding that "[a]fter sending a series of letters [to counsel for the person], including … one that warns of a consequence of a failure to respond, … the lawyer justifiably can conclude that she does not 'know' that the [person to be contacted] is represented by counsel." In that instance, the lawyer may therefore proceed to contact that person directly. Nevertheless, the opinion cautions that, when contact is made, the lawyer must advise the person that, if indeed he/she is represented by counsel, he/she should refer the communication to that counsel. *Id.*

What If the Other Party Initiates Contact with You?

The Rule applies regardless of how the possible communication arises. It does not matter if the other party initiates it, requests it, consents to it or tells the lawyer he/she does not feel the need to have his lawyer included. As Comment 3 to the New York Rule provides, "[a] lawyer must immediately terminate communication with a party if after commencing communication, the lawyer learns that the party is one with whom communication is not permitted by the Rule."

More complex is when someone whom the lawyer does not know to be a party or who was formerly connected to a party contacts the lawyer unsolicited with an offer of information about the matter in which the lawyer is involved. NYSBA Opinion 700 (1997) cautions the lawyer to proceed carefully and conservatively in that situation, lest they unintentionally get information (such as privileged information or work product) to which they are not entitled. There, an attorney prosecuting an administrative proceeding received an unsolicited telephone call from a person who said he was former non-lawyer employee of the law firm representing the respondent and had important information that thought the lawyer should know. *Id.* The lawyer sought guidance regarding how he should proceed. *Id.* The Committee advised that, although the contact was unsolicited, the lawyer still had the duties articulated in the predecessor of Rule 4.2 and related rules, particularly not to seek or obtain confidential information where disclosure might breach obligations to the other side. *Id.* Therefore, the Committee agreed that it was appropriate and advisable to seek guidance from "the tribunal [in which the matter is pending] or other appropriate authority" (such as another court) before accepting and reviewing the proffered information; so that the informer's status and the nature of the information could first be effectively and properly determined. *Id.*

As Opinion 700 indicates and as will be discussed further in Part II of this article, the desire to protect against unwarranted disclosure and use of privileged and confidential information is at the heart of Rule 4.2. *Id.* That is consistent with the rules and the majority of case law that generally require a lawyer who has received privileged or confidential information that he/she should not have been sent to advise the other party involved and not use the information without consent. *See e.g.*, NYRPC Rule 4.2(b); Fed. R. Civ. P. 26(b)(5)(B).

But, some other opinions do not necessarily apply Rule 4.4 when the information is unsolicited and the disclosure does not appear to be the result of inadvertence. For example, ABA Formal Opinion 06-440 (2006) cautions that Rule 4.4(b) applies only to documents inadvertently sent to a lawyer. Thus, Opinion 06-440 concludes that a lawyer who has received materials or information

which were "not the result of the sender's inadvertence" is "not required to notify another party or that party's lawyer." *Id.* Rather, that Opinion concludes, consistent with NYSBA Opinion 700, what action the lawyer should take is "a matter of law beyond the scope" of ethics rules (indeed one of "substantive law, at least in the first instance") for a court. NYSBA Comm. Prof. Eth., Op. 700 (1997).

When Is Contact 'Authorized … by the Law'?

The phrase "unless authorized … by the law" in Rule 4.2 does not conceal a secret key or otherwise hidden exception. NYRPC Rule 4.2. Rather, it is intended to clear the way for contacts such as lawful service of process, taking of a deposition or requesting documents, and other communications sanctioned or ordered by the court. *Id.* It also allows, in criminal matters, undercover operations and other such investigations. *Id.*

Even with such matters, lawyers should use care to avoid an improper conversation if the person involved is known to be represented by counsel. For example, in NYSBA Opinion 894 (2011*)*, the Committee cautioned that, while Rule 4.2(a) is not intended to prevent service of an eviction notice by a landlord, the person doing so (and particularly one who is not a professional process server) should not use the occasion to engage in conversation that would otherwise be barred by the Rule. That means not discussing anything of substance related to the legal matter involved beyond confirming that the person being served is the one intended to be served. *Id.*

An interesting recent opinion of the New York County Lawyers Association, Opinion 745 (2013*)*, discussed further in Part II, noted that lawyers are increasingly using the "unless authorized by law" exception to seek court-ordered access to password protected social media of parties and others whom they wish to contact. *See infra* Part II.

Does Lawyer Have Duty to Inquire Whether Person Has Counsel?

Rule 4.2 prohibits contact when a lawyer "knows" that a person is represented by counsel. NYRPC Rule 4.2. It does not say "has reason to know;" and Rule 1.0(k) defines knowledge as "actual knowledge of the fact in question." NYRPC Rule 1.0(k). But, Rule 1.0(k) adds that "knowledge may be inferred from the circumstances." *Id.*; s*ee also,* NYRPC Rule 4.2 cmt. 8. Thus, as a general proposition, a lawyer does not have a duty to inquire as to whether a person to be contacted is represented by counsel; but the lawyer cannot "turn a blind eye" to that question. As explained in NYSBA Opinion 728 (2000), "in some circumstances, a lawyer must confirm that an individual is not represented by counsel in the particular matter before communicating directly with the individual." For example, if the person was known to have been represented previously, and it's reasonable to think that may still be the case, inquiry should be made. *Id.*

Other situations might exist where a lawyer knows that the person had counsel on a similar or even unrelated matter or is someone who generally deals with legal matters through or with

counsel. There, a lawyer has reason to believe the person may have counsel in the current instance. *See, e.g.*, NYSBA Comm. Prof. Eth., Op. 904 (2012) (possible civil action against person who was represented by counsel in criminal fraud investigation concerning the same situation.) More troublesome is what the lawyer must or can do if it becomes apparent *during* the conversation that the person is represented by counsel or may want to be. If that occurs, the lawyer should ask if the person wishes to continue to speak with her or would prefer to do that through her counsel.

Communicating with unrepresented persons poses a further set of issues. This is addressed in New York Rule 4.3 and the Comments to that Rule. Essentially, they require that the lawyer properly identify himself, and take care to ensure that the person does not incorrectly believe he is disinterested, or otherwise misunderstands or miscomprehends his role, and what he is asking. *Id.*; *see also,* N.Y. Cty. Law. Assn., Op. 708 (1995). The Rule also prohibits the lawyer from giving legal advice to an unrepresented person, although that too is subject to exceptions. [NYRPC Rule 4.3.] For example, the lawyer may have the responsibility in some instances, to advise the person to consider getting legal counsel. *See,* NYC Bar Assn. Comm. Prof. Jud. Eth., Op. 2009-2 (2009) for guidance in that regard. “[T]he general rationale” of the no-contact rules is that “[t]the legal system in its broadest sense functions best when persons in need of legal assistance or advice are represented by their own counsel.” NYSBA Comm. Prof. Eth., Op. 728 (2000), quoting Ethical Consideration 7-18).

Therefore, a lawyer is well-advised to keep in mind not only the letter of the Rule but also its purpose and spirit whenever considering whether he can or should communicate with someone who is not represented by counsel. For example, in *In re Winiarsky,* 104 A.D.3d 1, 9-10 (N.Y. 1st Dept. 2012), the court censured counsel for obtaining affidavits from potential witnesses who contacted him and asked if they could give testimony without having to appear in court. The court there was troubled that the witnesses may not have understood that they didn’t have to give testimony at all or that they could answer only some questions and not others *Id.* at 4. To better understand these rules and limitations, *see,* “Simon’s Overview of Rule 4.3” in *Simon’s Rules of Professional Conduct*, 1230 (2014).

What Are the Consequences If a Lawyer Violates the Rule?

Failure to adhere to the no-contact rule can have serious consequences for counsel, as well as for her client. Disciplinary authorities have full power to act in response as they deem warranted by the nature and extent of the violation of Rules of Professional Conduct. *See, e.g.*, *In re Matthew B. Murray,* 2013 WL 5630414, No. 11-070-088405, at *1 (2013); *Winiarsky*, 104 A.D.3d at 9-10. In addition, courts may impose their own sanctions. *See,* NYSBA Comm. Prof. Eth., Op. 700 (1997); *Maldonado v. New Jersey,* 225 F.R.D. 120, 133 (D. N.J. 2004). Counsel and his/her law firm may also be disqualified from continuing in the matter. *See, e.g.*, *Acacia Patent Acquisition, LLC v. Superior Ct.,* 2015 WL 851517, No. G050226, at *1 (Cal. Ct. App. 2/27/2015). Or short of that, the court may suppress evidence that might otherwise be admitted if properly obtained, or otherwise limit and restrict what may be said about it. *See, e.g.*, *Fayemi v. Hambrecht & Quist Inc.,* 174 F.R.D. 319, 323-25 (S.D.N.Y. 1997); *U.S. v. Hammad,* 858 F.2d 834,

237 (2d Cir. 1988).

Also, as explained above, counsel may unwittingly have created her own attorney-client relationship with the person involved, with all the attendant duties and responsibilities that entails. Even without that, counsel may have assumed unwanted duties of non-disclosure.

Recognizing these consequences, an attorney should understand what the Rule expressly prohibits, as well as the purpose of the Rule. Depending on the circumstances, the reach of the rule may be unclear.

As noted, Part II of this article will address other aspects and application of the no-contact rule and some situations that lawyers often encounter. That discussion will attempt to provide further practical guidance on how lawyers can avoid running afoul of the Rule.

Martin I. Kaminsky is General Counsel of Greenberg Traurig LLP. Prior to taking that position, he was trial and appellate counsel in cases involving securities, commodities, antitrust, corporate, contract, discrimination, legal malpractice and other business litigation issues.

Maren J, Messing is an associate at Patterson, Belknap Webb & Tyler LLP, involved in a variety of cases. Prior to joining that firm, she clerked in the federal district and appeals courts in New York.

Get CLE Credit for this month's articles (April 2015).

« "Illegal" Conduct Under Rule 1.2: When Does Advice to a Client Violate an Attorney's Ethical Obligations? "Remembering Professor Monroe Freedman" »

The Use of Investigators in IP Matters

prepared for

NYSBA IP Section Spring Meeting

by

William B. Belmont, Esq.
The Belmont Group, LLC

Investigative Techniques

- Ethical Investigations
- Research
- Theft of Trade Secrets
- Field Investigations
- Asset Searches
- International Work
- Thinking Outside the Box

Ethical Investigations

- KYI
- Investigator as Customer Services Representative
- No Contact Rule - Agency Restrictions
- Poisonous Tree Doctrine
- Social Engineering v. Pretexting (Fraud)

Research

- Background Information
- Business Affiliations
- Litigation
- Property Records
- News and Media Searches
- Internet and Web Activity
- Criminal Records
- Government Agencies

Background Information

- Fully Identify an Individual
  - Government Identification
  - Accuracy Matters
  - Aliases
  - Maiden Names
  - Sr. Jr. III
  - Foreign Names
  - Spelling Errors
- Date of Birth
  - November 5th as 5/11
- Social Security Numbers

Background Information

- Address History
- Questionnaire and Release
- Corporations
  - Corporate Tax Identification Number

Business Affiliations

- Research Former and Current Associates
- Identify Previously Undisclosed Relationships
- Identify Vendors Suppliers Customers
- Hidden Assets
- Identify Silent Roles in Companies
- Expose Conflicts

Litigation

- Address History
  - County Only
- All Jurisdictions
  - Name Match Only
  - Federal, State and Local
- Active and Closed Lawsuits
  - Pleadings, Motions, Affidavits
- Judgments and Liens
  - Lead Generator

Litigation

- Bankruptcy Filings
  - Lead Generator
- Uniform Commercial Code ("UCC") Filings
  - Lead Generator
- Divorce Proceedings
  - Hell Hath no Fury
- Contact Litigation Adversary

Property Records

- Individual Holdings
  - Helps with Address History
- Potential Locations of Activities
  - Warehouse Counterfeiting example
- Lead Generator
  - Links to Associates or Businesses
  - Own or Lease Property
  - Roommates or Neighbors
- Asset Searches

News and Media Searches

- Tons of Potential Information
  - Name Commonality
- Newspapers, Magazines & Local Papers
  - Electronic Newspaper “comment section”
- General and Trade Publications
  - Name Commonality
- Personal & Social Information
  - Associations and Associates
  - Life Events

Internet and Web Activity

- Google
  - Employers and Colleges and Dating
- Social & Professional Networking Sites
  - Facebook and Instagram
  - Locate Information
  - Gym Rat
  - High School Reunion
- Great Place for Photo
- Employment Information

Internet and Web Activity

- Never Goes Away
- Comments and Blog
  - Lies can be Lead Generators
  - Nuggie example
- Ethical Alert
  - Facebook Friends

Criminal Records

- Statewide or County by County
  - Accurate Name and DOB
  - Disclosure Rules Vary
- Arrest or Conviction
- Police Reports and Court Files
- Sealed or Expunged
- Check for Photo

Government Agencies

- Federal, State, County and Local
- Lead Generator
  - Business Ownership
  - Regulatory Violations
  - Applications and Permits
  - Sanctions and Fines
- Patriot Act
- Sarbanes-Oxley Act
  - Anonymous Hotline

Theft of Trade Secrets

- Identifying Possible Means of Information Loss
- Establishing Access to Information
- Computer Error v. Human Error
- Vigilance v. Complacency
- Anonymous Hotlines

Field Investigations

- Surveillance
- Direct Contact Investigations
  - Witness Statements
  - Locate Investigations
  - Incident Scene Investigations

Surveillance

- Photo
- Considerations and Tactics
  - How many investigators
  - Google Maps
  - Urban v. Rural, Foot v. Car v. Mass Transit
  - Employment Information
- Video
  - When to and not to
  - Testify
- Report or No Report

Surveillance

- Confirm Address
  - DMV
- Budget
  - Half day v. Full day
  - Rome was not built in one day
- A Day in the Life
  - Surveillance Intel

Direct Contact Investigations

- Witness Statements
  - Customer Services Representative
  - Typo
  - Contact Information and Description
  - Signature or No Signature

Direct Contact Investigations

- Locate Investigations
  - Clients and Witnesses
    - Cases take years
    - Get good initial info
  - Adversary

Address easier than Phone

Direct Contact Investigations

- Incident Scene Investigations
  - Photos and Measurements
  - CCTV
  - Incident Reports
  - Witness Canvass
    - Same Day and Time
    - Poster

Asset Searches

- Asset Profile
  - Judgments and Liens
  - Bankruptcy Filings
  - UCC Filings
  - Property
  - Cars, Planes and Boats
  - Stocks
  - Tangible Assets
- Financial Assets
  - Pre or Post Judgment
- Domestic and International

International Investigations

- No one has as much info as the US
- Specific to Region and City
- FCPA
- Privacy

Thinking Outside the Box

- who Knows what you want to Know
- Technology
  - GPS
  - Cell Phone Pinging
  - Drones
  - LPR
- Traditional
  - Investigators Testimony
  - Dumpster Dives
- Ethics
  - Cell phone records

Questions?

William B. Belmont, Esq.
The Belmont Group, LLC
118 East 60th Street, Suite 2100
New York, New York 10022
Direct: 212.695.0086
Fax: 917.591.3361
Email: bill@thebelmontgrp.com
www.thebelmontgrp.com

Artificial Intelligence and the Law – A Primer for Lawyers. Will We All Become Obsolete?

Rory Radding (Moderator)
Partner, Locke Lord LLP

Alexander Puutio (Moderator)
Administrative Officer, United Nations

Diane Holt
Team Lead – Transactions, Bloomberg Law – Introduction to AI

Jonathan Askin
Professor, Brooklyn Law School – AI, IP and Legal Tech

Matthew D'Amore
Associate Dean, Cornell Tech – AI in Law Practice and Legal Education

Ned Gannon
President, eBrevia – Application of AI in the Legal Profession

Locke Lord LLP

New York State Bar Association
IP Section Spring Meeting
April 5, 2019

The Pitfalls, Problems and Impact of Artificial Intelligence on IP Rights: Inventorship, Ownership and Infringement

Rory Radding

Partner, Locke Lord, LLP

New York, New York, U.S.A.

Rory.Radding@lockelord.com

Overview

- **Definitions** - Many definitions exist but a workable definition is from the Association for the Advancement of Artificial Intelligence
  - "the scientific understanding of the mechanisms underlying thought and intelligent behavior and their embodiment in machines." See www.aaai.org

Overview

- Types of AI
  - Machine learning
  - Neural networks
  - Deep learning
  - Search
  - Probabilistic reasoning
  - Prediction

Overview

- **A Little History**
  - 4th century BC – Aristotle invented syllogisitc logic, the first formal deductive reasoning system.
  - 13th century – in 1206 A.C., Ismail Al-Jazari, an Islamic scholar and prolific automation inventor, designed a programmable humanoid robot – a boat carrying four mechanical musicians powered by waterflow
  - 1926-1940 – Alan Turing proposes the universal computing machine (0's and 1's)
  - 1950 – Turing publishes "Computing Machinery and Intelligence" (mimic human behavior)
  - 1950s – Algorithms play checkers and image recognition
  - 1956 – John McCarthy created the term "artificial intelligence" at Dartmouth
  - 1959 – Arthur Samuel (IBM) coins "machine learning"

Overview

- **A Little History**
  - 1962 – First industrial robot company, Unimation, founded
  - 1966 – semantic nets created
  - 1969 – First International Joint Conference on Artificial Intelligence in Washington, D.C.
  - 1974 – First expert system
  - 1978 – “satisficing” decision making,
  - 1979 – “Stanford Cart”: First computer controlled autonomous vehicle
  - 1981 – Danny Hillis connection machine – parallel computing. He later founds Thinking Machine, Inc.

Overview

- **A Little History**
  - 1990s to the present - Major advances in all areas of AI, with significant demonstrations in machine learning, intelligent tutoring, case-based reasoning, multi-agent planning, scheduling, uncertain reasoning, data mining, natural language understanding and translation, vision, virtual reality, autonomous vehicles, games (chess, checkers, Go) and other topics, some using IBM’s Deep Blue.
  - 2006 – Geoffrey Hinton coins “deep learning” – multilayer neural networks.
  - 2010 – Siri personal assistant
  - 2011 – IBM’s Watson
  - 2014 – Amazon’s Alexa

Patents

- Basic Concepts
  - Has the invention been created autonomously by the AI system?
    - AI generated invention
    - AI enabled invention

Possible actors in producing/creating inventions

- software programmers
- creator of the AI algorithm but may not focus on the application of the AI system
- data suppliers -- AI system sifts through data to learn
- checkers of AI system results to correct them, if necessary
- owner of the AI system, e.g., IBM owns Watson
- operators -- licensee or service provider
- public
- government
- investor
- the AI system itself

How to Identify the Actual Owner of AI Patent Rights?

- First Must Identify Inventor
  - Because conception is the touchstone of inventorship, **each joint inventor must generally contribute to the conception of the invention**.
  - Conception is the "formation in the mind of the inventor, of a **definite and permanent idea of the complete and operative invention**, as it is hereafter to be applied in practice."
  - Joint inventors must be "**aware**" of each other's work on the invention. If they have had no contact whatsoever and are completely unaware of each other's work, they cannot be joint inventors.
  - Merely adding **routine** knowledge, well-known principles", techniques, or skill is **not** an inventive contribution.

Then Who is the Owner?

- Ownership initially vests in each **inventor**, absent an agreement to the contrary.
- Each co-owner's ownership rights carry with them the **right to license others**, a right that also does not require the consent of any other co-owner.
- Ordinarily, one co-owner has the **right to impede the co-owner's ability to sue infringers** by refusing to voluntarily join in such a suit.

Who Can infringe?

- Usually need some form of human involvement
  - U.S. patent law states “whoever” makes, uses, sells, offers for sale or import.
  - Computer owner, developer and user are different entities.
- Joint Infringement
  - System or Apparatus
    - infringing use does not require a party to exercise physical or direct control over each individual element of the system. **The party collecting the information may still be said to be using the system** because if the user did not make the request, then the processing would not be put into service demonstrating ‘**control**’ of the system.
    - But not owning or directly controlling the AI may not be sufficient to avoid infringement.

Locke Lord

11

Who Can Infringe? (continued)

- Method
  - Consider who is designing, controlling, and owning the AI.
  - Infringement outside the U.S. by AI system or apparatus located and operated outside U.S. if control exercised there.
  - Infringe inside the U.S. for a method since all steps must be performed in U.S.
  - Inducing infringement
    - Knowingly causes another to infringe and knowing the other will infringe
- Can a computer infringe?
  - If human owns AI then human infringer.
  - But AI learns and modifies to produce a product as action -- is the owner still the infringer?
  - Is the AI an inducer?

Locke Lord

12

Copyright

- An original work of authorship fixed in any tangible medium of expression, now known or later developed from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device

The Basic Question: Is a work of authorship created solely by a machine using AI an "original work of authorship"?

- The cases break into two answers:
  - Would instructing the machine as to what areas you want it to create be sufficient?
    - Under U.S. law, the Copyright Office has accepted such works as being "works of authorship", entitled to copyright protection.
  - What if the machine does all of the creation itself, as an independent actor without additional human instruction?
    - Under U.S. law, the Copyright Office has rejected such works as not having sufficient "human authorship" to qualify for registration
    - Such works now fall into the public domain and are unprotectable under law.
  - How does this impact foreign created works copyrighted under the laws of other countries?
    - Registration for such works is not required in the United States for them to be enforceable so it will be a matter for U.S. Courts.
- The practical use of such AI technologies today and in the future in creating what are now copyrighted works if made by humans suggest Copyright law reform is necessary.

Human Must Create Copy Work

- Naruto v. Slater (2016)
  - Naruto, a crested macaque, took a selfie using David Slater's camera
  - Slater published the photographs
  - Naruto, through People for the Ethical Treatment of Animals, sued Slater for infringing Naruto's copyrights in the photos
  - The Court dismissed the case, finding Naruto not the "author" under the Copyright Act – not human

Copyright and Artificial Creativity By Territory

- May the works of artificial intelligence be copyrighted?
  - No: the USA, the EU, Canada, Australia, Singapore
    - The obstacle generally lies in the requirement of human author
  - Yes: the UK, Ireland, New Zealand, Hong Kong, India
  - However, even where copyrights may subsist, the law may treat AI –generated works differently:
    - Different duration (UK and HK)
    - Moral rights (such as the right to be identified as the author)

Should We Grant Copyright/Patents to AI Created Works?

- Two major rationales:
  - 1. The functional, utilitarian approach: copyrights granted in order to "promote the progress of Science and the useful Arts"
    - Generally accepting of artificial creativity, as long as society benefits in the end.
  - 2. The moral-rights approach: copyrights are granted in order either to recognize the labor of the artists or because creative works are an expression of individualism and identity, and are thus protected as part of the creator's essential personhood
  - 3. Possible compromise: some jurisdictions which grant copyright to AI works nonetheless grant them different moral rights

Who painted this painting?

Who is the Author of this AI-created poem?

"The crow crooked on more beautiful and free,
He journeyed off into the quarter sea.
His radiant ribs girdles empty and very- lease
beautiful as dignified to see"

Where do we go from here?

- Questions with no easy answers:
  - 1. What is creativity, what is its purpose, and who should benefit from it?
  - 2. What is the relationship between creativity, personhood, and humanity?
    - Are they inextricably linked, or may emerging AIs independently possess some of these traits selectively?
    - What might the policy considerations be to "outsourcing" elements of creativity to AIs?
  - 3. If an AI possesses sufficient creativity and personhood to be the author of an original work, do ethical concerns arise regarding the creation and exploitation of such AIs?
  - 4. Without patent or copyright, how will the investment in these technologies be recouped?

Questions??

THANK YOU!

Rory J. Radding
Partner
Locke Lord LLP
New York, New York, U.S.A.
rory.radding@lockelord.com

Locke Lord

AI & the Law: A Primer

NYSBA Emerging Trends Program

Diane Holt, Team Lead – Transactions
April 5, 2019

Bloomberg Law

Computing Machinery and Intelligence (A.M. Turing)

Bloomberg Law

The Imitation Game

I propose to consider the question, “Can machines think?”

…

An important feature of a learning machine is that its teacher will often be very largely ignorant of quite what is going on inside, although he may still be able to some extent to predict his pupil’s behavior.

Three Critical Questions to Focus Your Analysis

1. What Type of “Artificial Intelligence” Are We Talking About?
2. What Laws Impact Instance of AI?
3. What’s the Problem We’re Trying To Solve?

1. What is Artificial Intelligence?

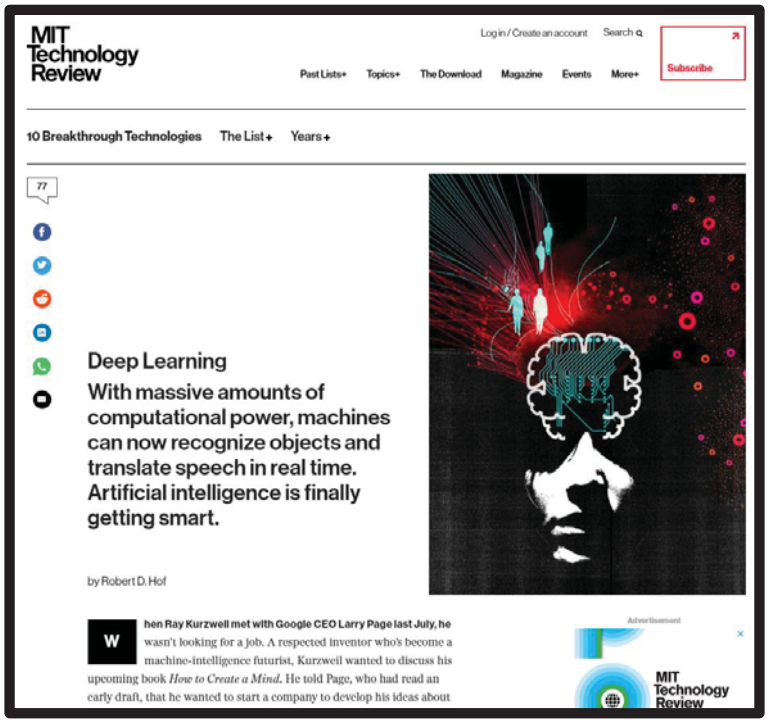
Bloomberg Law

Artificial intelligence is an advanced technology that allows a computer to develop its own program by learning from data.

- **Algorithm** = formula; hard coding an output; line-by-line coding; rules
  - Example: credit score
- **Machine learning** shifts burden of program-writing to the computer
- **Supervised learning** uses training data so that a computer can develop inferences. More data = more accuracy. Uses some or all labeled data.
  - Example: credit card fraud screening; “you might like”
- **Deep Learning**
  - Examples: analyzing faces; CT scan study (The Lancet, December 1, 2018), Google’s Deep Mind, Stock Fish, chess

Why Now? Computing Power

Bloomberg Law



MIT Technology Review

Log in / Create an account Search

Past Lists+ Topics+ The Download Magazine Events More+

Subscribe

10 Breakthrough Technologies The List+ Years+

77

Deep Learning

With massive amounts of computational power, machines can now recognize objects and translate speech in real time. Artificial intelligence is finally getting smart.

by Robert D. Hof

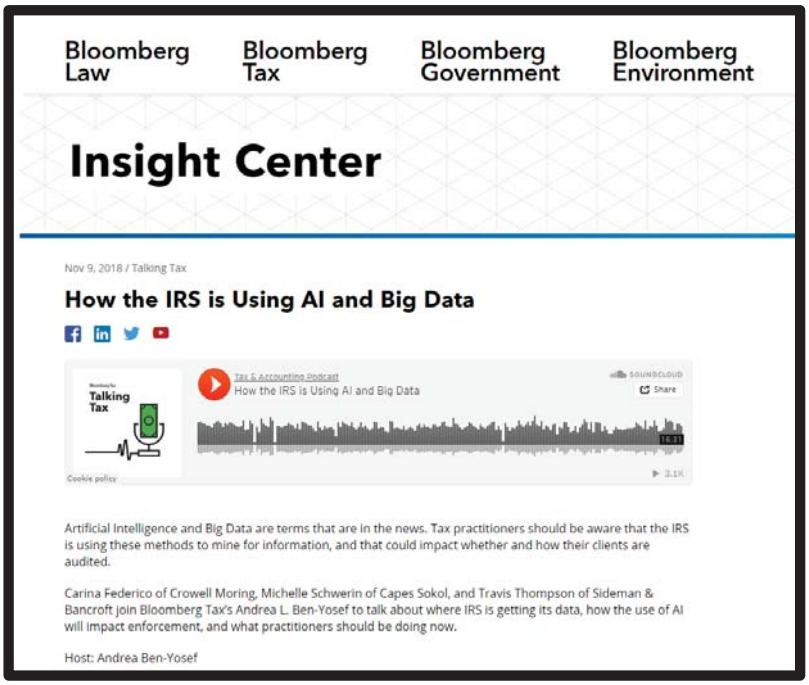
When Ray Kurzweil met with Google CEO Larry Page last July, he wasn't looking for a job. A respected inventor who's become a machine-intelligence futurist, Kurzweil wanted to discuss his upcoming book *How to Create a Mind*. He told Page, who had read an early draft, that he wanted to start a company to develop his ideas about

Advertisement

MIT Technology Review

Why Now? Big Data

Bloomberg Law



Bloomberg Law | Bloomberg Tax | Bloomberg Government | Bloomberg Environment

Insight Center

Nov 9, 2018 / Talking Tax

How the IRS is Using AI and Big Data

Tax & Accounting Podcast
How the IRS is Using AI and Big Data
SOUNDCLOUD
Share
Talking Tax
Cookie policy

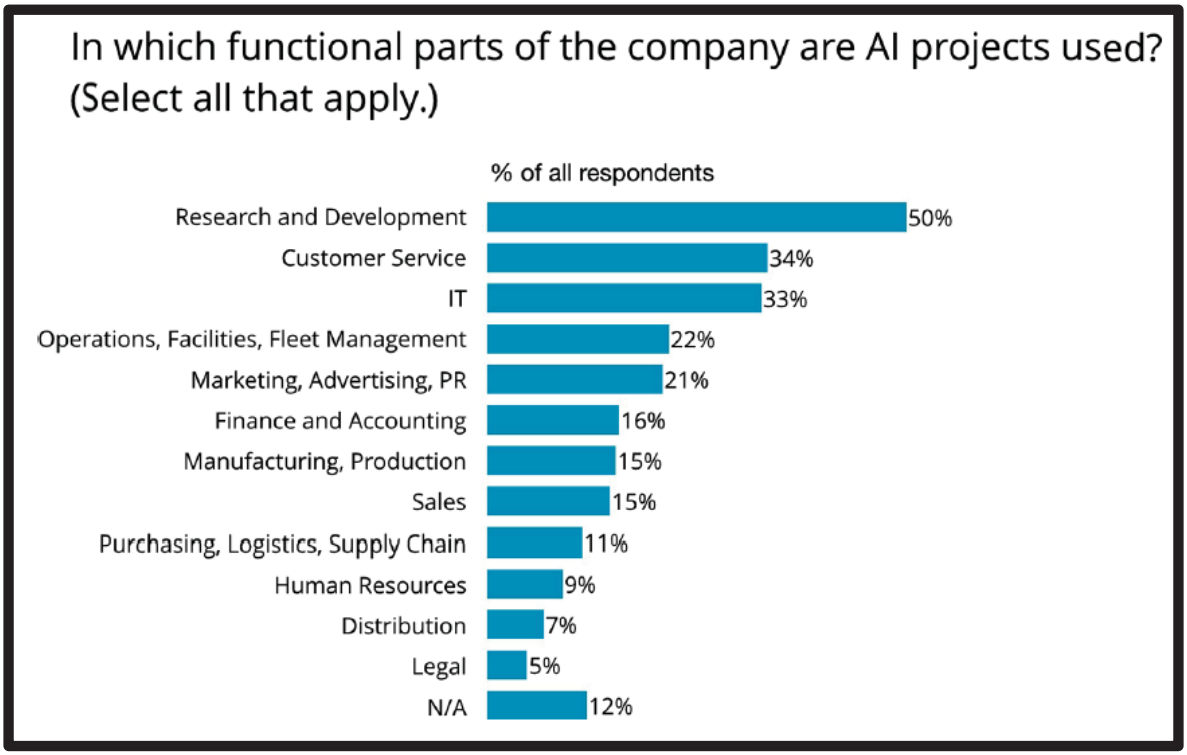
Artificial Intelligence and Big Data are terms that are in the news. Tax practitioners should be aware that the IRS is using these methods to mine for information, and that could impact whether and how their clients are audited.

Carina Federico of Crowell Moring, Michelle Schwerin of Capes Sokol, and Travis Thompson of Sideman & Bancroft join Bloomberg Tax's Andrea L. Ben-Yosef to talk about where IRS is getting its data, how the use of AI will impact enforcement, and what practitioners should be doing now.

Host: Andrea Ben-Yosef

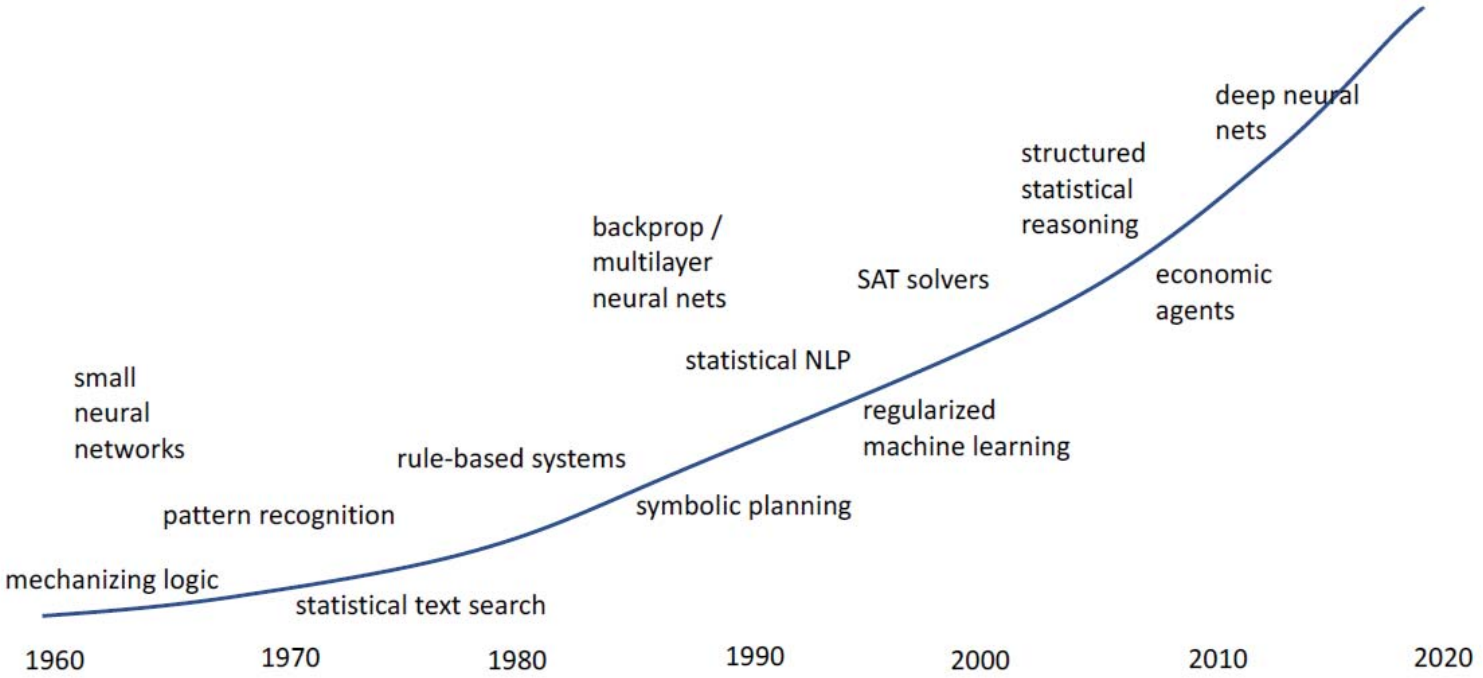
AI Adoption in the Enterprise (O'Reilly)

Bloomberg Law



Technical Progress in AI (Dave Lewis, Brainspace)

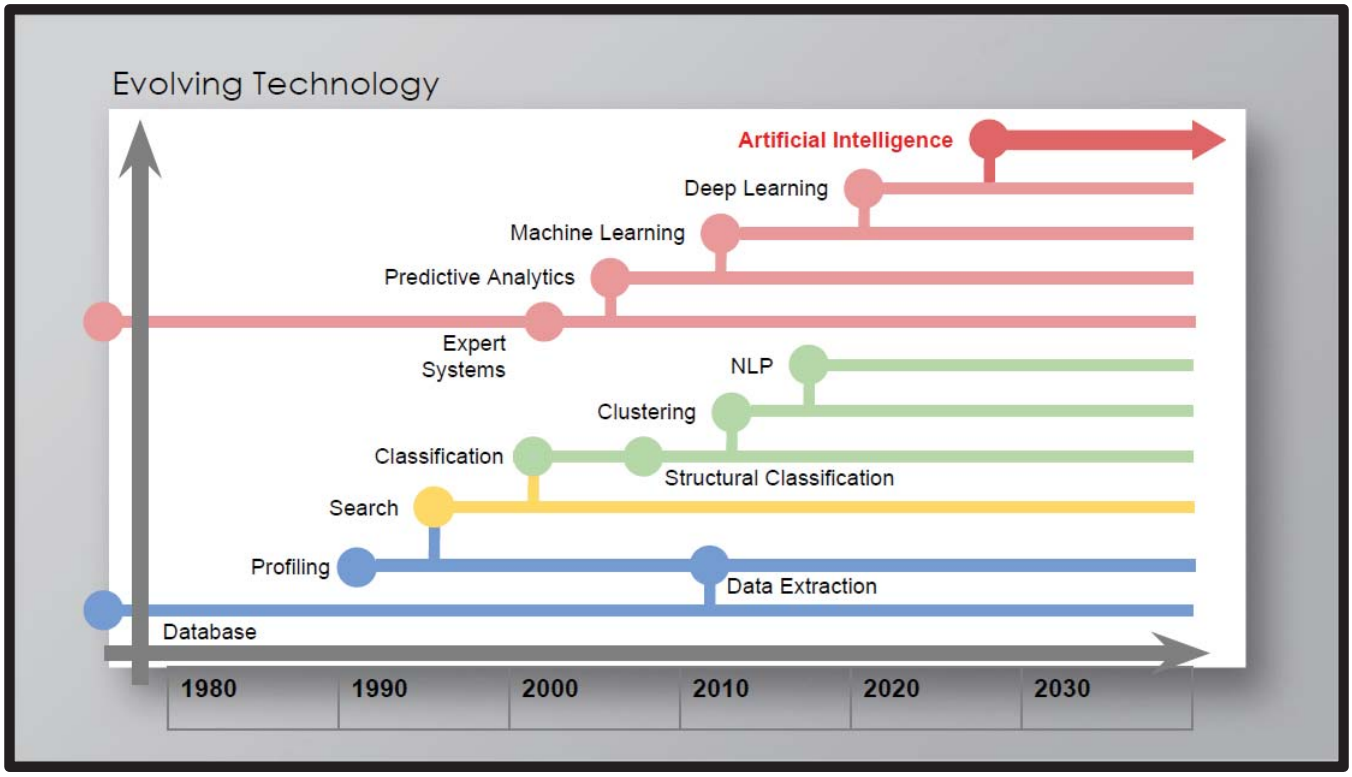
Bloomberg Law



Brainspace

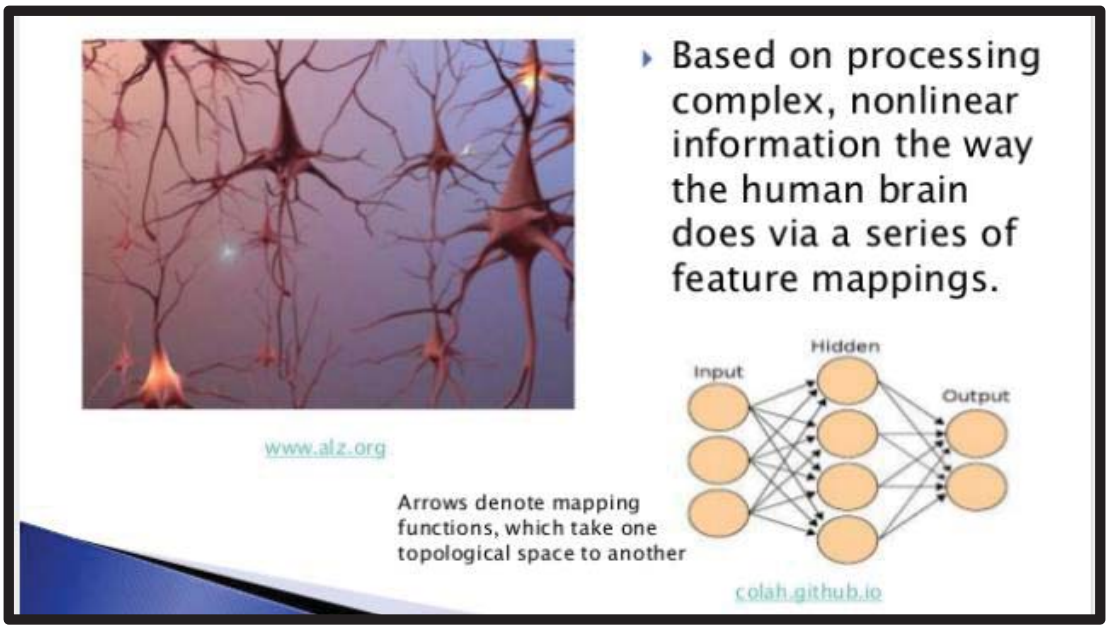
Evolving Technology (Kingsley Martin)

Bloomberg Law



Neural Networks (Colleen Farrelly, Kaplan)

Bloomberg Law



Neural Networks (Colleen Farrelly, Kaplan)

Bloomberg Law

- Added layers in neural network to solve width problem in single-layer networks for universal approximation.
- More effective in learning features of the data.
- Like sifting data with multiple sifters to distill finer and finer pieces of the data.
- Computationally intensive and requires architecture design and optimization.

2. Legal Principles Applying to AI

Bloomberg Law

- Ethical rules – which may constrain the use of AI – or require it
  - Model Rules 1.1 (competence), 2.1 (independent judgement), confidentiality (1.6), 5.1 & 5.3 (supervise)
- Statutes and regulations
- Case law

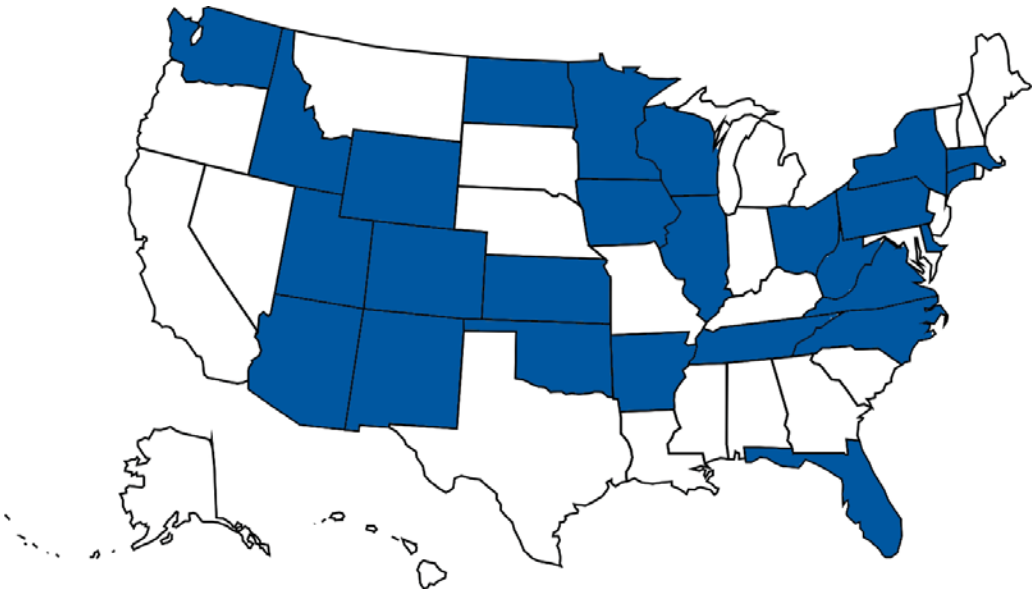
  ➢ Understanding the technology itself is critical to understanding compliance

ABA Model Rule 1.1 cmt 8

Bloomberg Law

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.



Some Existing Legal Frameworks

Bloomberg Law

- Prohibiting discrimination
  - Equal Credit Opportunity Act
  - Fair Housing Act
- Prohibiting unfair or deceptive acts or practices
  - Federal Trade Commission Act, section 5
  - Dodd-Frank Wall Street Reform and Consumer Protection Act
  - Many state laws
- Employment Laws
  - Federal and State
- Privacy Laws
  - California Consumer Privacy Act (effective January 1, 2020), creates consumer right to privacy and right of action for damages
  - Hawaii, Illinois, Maryland, Massachusetts, New Jersey, New Mexico, New York, Rhode Island, Texas and Washington

GDPR

Bloomberg Law

European Union’s General Data Protection Regulation, effective May 25, 2018

- Article 22: “The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.”
- Recital 71: “Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.”

3. What's the Problem We're Solving?

Bloomberg Law

Moving from Hype to Savvy

- What is the stated purpose of the tool?
- Why do we want the tool?
  - Efficiency? Insights? Cost savings? Additional billings?
- How does the tool work?
  - What is the dataset over which it runs?
  - How effective is the tool?
- How will we use the tool?
  - How will we confirm its effectiveness?
- Is it meeting our objectives?
  - How do we know it is?

Machines Practicing Law?

Bloomberg Law

[A]n individual who, in the course of reviewing discovery documents, undertakes tasks that could otherwise be performed entirely by a machine cannot be said to engage in the practice of law.

> Lola v. Skadden, Arps, Slate, Meagher & Flom LLP, 620 Fed. Appx. 37, 45, 2015 BL 235274, 8 (2d Cir. 2015)

- Michael Simon says that this case represents “the first federal appellate court to draw a distinction between the roles of person and machine in the ‘practice of law.’”

Lola v Skadden and the Automation of the Legal Profession

Bloomberg Law

1. Design and create the machine's thinking
2. Provide big-picture perspective
3. Integrate and synthesize across multiple systems and results
4. Test and monitor
5. Know how to best apply the system
6. Elicit the necessary information
7. Persuade humans to take action on automated recommendations

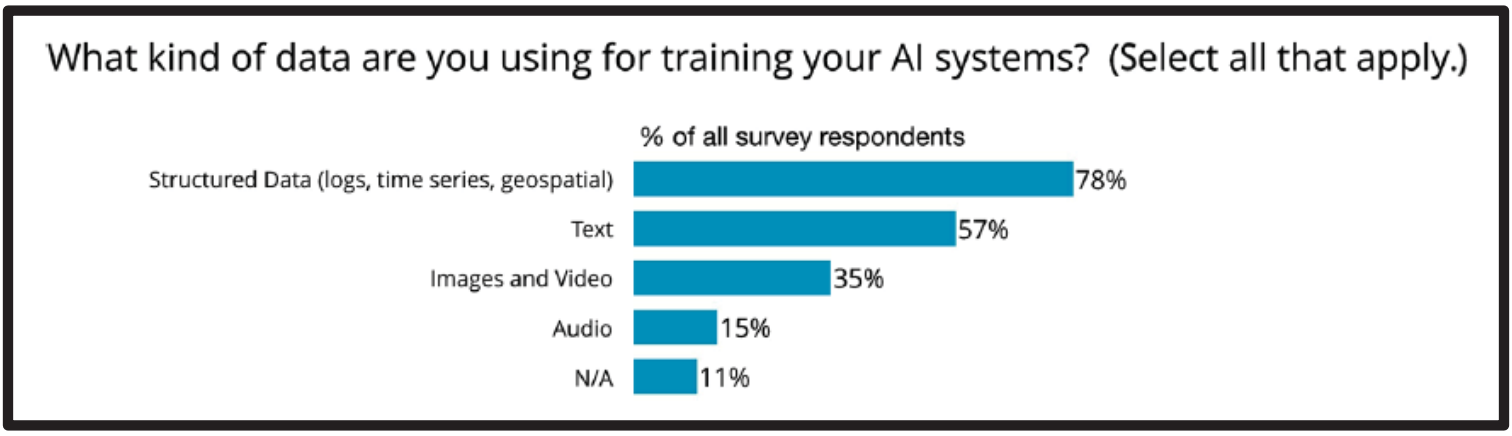
Michael Simon, Alvin F. Lindsay, Loly Sosa & Paige Comparato, 20 Yale J.L. & Tech. 234 (2018) (citing and quoting Only Humans Need Apply by Thomas Davenport & Julia Kirby).

AI Tool to Research the AI Legal Principle

Bloomberg Law

Sources of Training Data by O'Reilly

Bloomberg Law



Don’t Forget to Evaluate the Data

Bloomberg Law

- Each data point
  - Is each data point relevant to the task?
  - If there is no nexus with the principle being examined, is there legal risk?
  - Example: Is zip code relevant to creditworthiness?

- Inferences from the dataset
  - Does the entire set of data contain problems that will be magnified? Will the data change over time?
  - Are the data accurate, reliable and representative? Have they been validated for the purpose at hand?
  - Example: Historical employment demographics vs desired employment demographics

See, e.g., “Keeping Fintech Fair: Thinking About Fair Lending and UDAP Risks,” by Carol A. Evans (Consumer Compliance Outlook, Second Issue 2017). See also “Accountable Algorithms,” by Joshua A. Kroll et al. (U. Penn. L. Rev. 2017).

Moving Toward Audits

Source: BDO USA

Diane Holt

Team Lead – Transactions
Bloomberg Law

Dholt@BloombergLaw.com

AI and the Next Gen Lawyer

Prof. Jonathan Askin
Brooklyn Law School
Founder/Director, Brooklyn Law Incubator & Policy Clinic
Faculty Chair and Innovation Catalyst, Center for Urban Business Entrepreneurship
Visiting Professor, MIT
@jaskin

CUBE
Brooklyn Law School Center for Urban Business Entrepreneurship

Brooklyn Law School est1901

Blip CLINIC

LTL
Legal Technology Laboratory

LEGAL HACKERS

iLINC

Brief History of the Evolution of Law and Technology (not to scale)

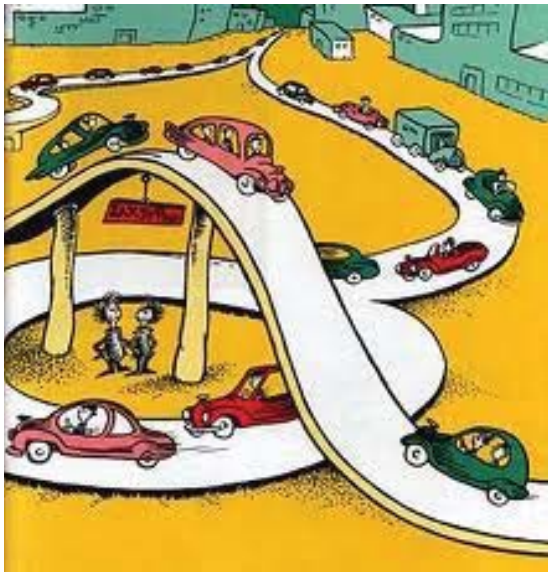
British Middle Ages → Acceleration in 19th Century → Innovation in 20th Century → Internet-Enabled Future

General Legal Regimes — Industry-Specific Legal Regimes

Common Law	Statutory Law	Administrative Law	Inflection Point Like We Have Never Seen Before
New issues/needs:	**New issues/needs:**	**Establishment of:**	-Internet Governance
Property	**Corporations**	**ICC**	-Technical Standards
Contracts	**Consumer Protection**	**SEC**	-Openness/Transparency
Torts	**Copyright** (for analog world)	**FCC**	-Accountability
Common Carriage (transport carriers and public houses)	**Antitrust**	**FTC**	-Privacy
Public Utilities		**State Agencies**	-Security
			-Jurisdiction
			-Online liberties/rights
			-Government services
			-Political process
			-Innovation policy
			-Sharing Economy
			-Economic/Social progress
			-Transactions
			-IPR / Digital Rights
			-Big Data
			-Algorithmic Law
			-Blockchain

3

Zax Bypass: Lawyers as Roadblocks



4

A Young Lawyer Learns the Entrepreneur's Lesson the Hard Way

FWD®

skype™

Lawyers as Enablers

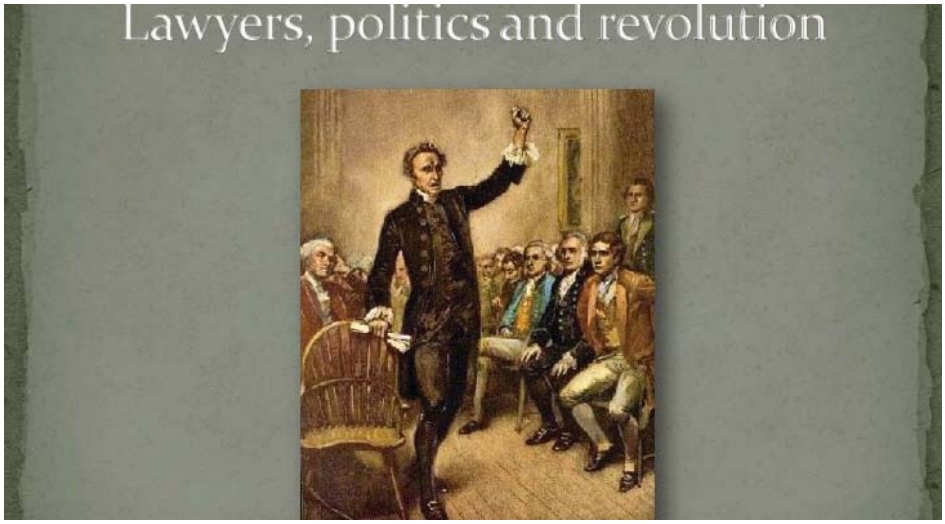
IN A

HERE'S HOW:

eversign

docracy

7



9

The Lawyer's Role?

10

The Future of Lawyers

- *"The future is here already, it's just not evenly distributed."* - William Gibson
- Need for legal minds greater than ever
  - Legal processes and rules and implications of emerging world
  - Haven't figured out how to deploy

11

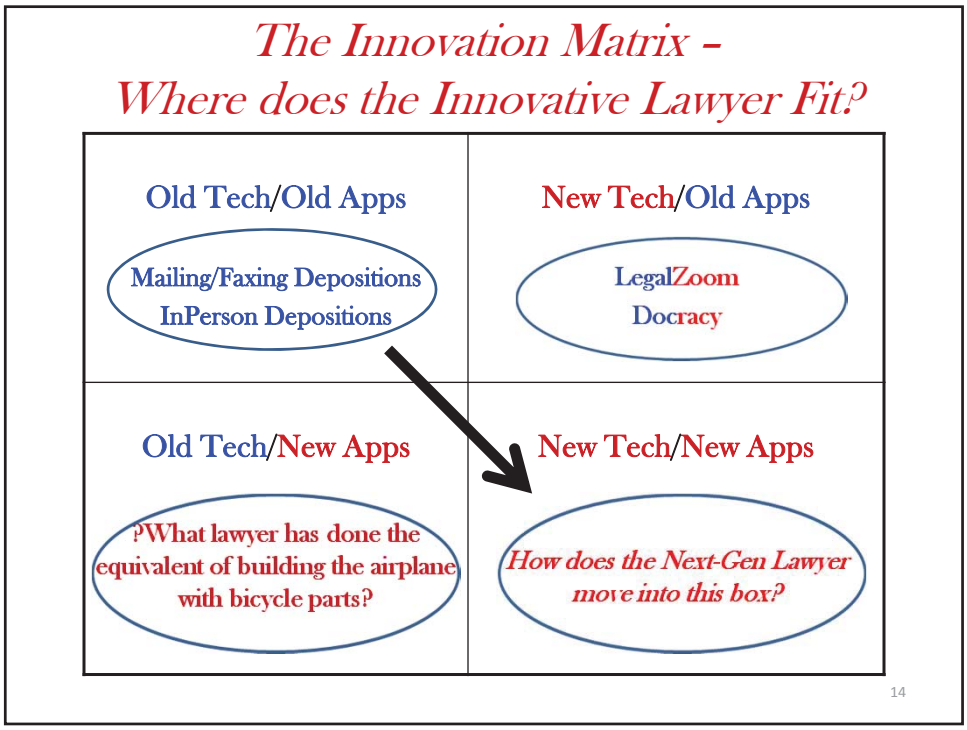
Arthur C. Clarke's three "laws" of prediction:

1) When a distinguished but elderly scientist states that something is possible, he is almost certainly right. When he states that something is impossible, he is very probably wrong.

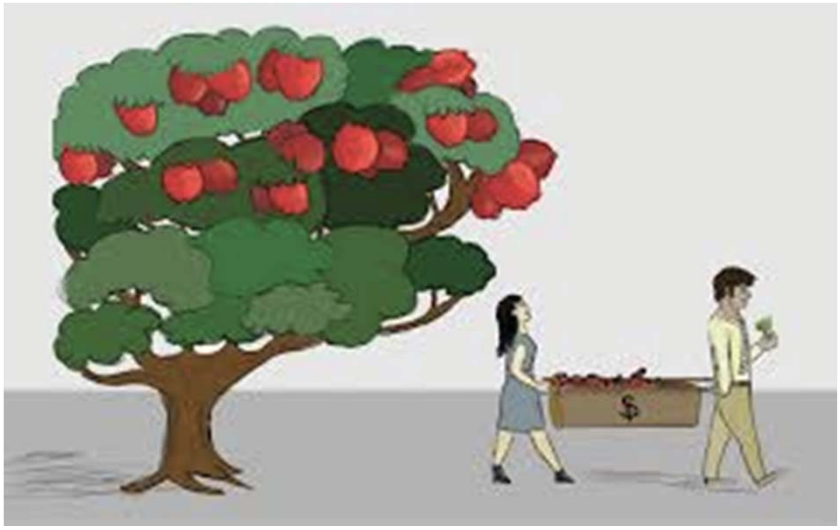
2) The only way of discovering the limits of the possible is to venture a little way past them into the impossible.

3) Any sufficiently advanced technology is indistinguishable from magic.


LEGAL HACKERS
iLINC
STARTUP AMERICA PARTNERSHIP
LTL
Legal Technology Laboratory
mit media lab
13

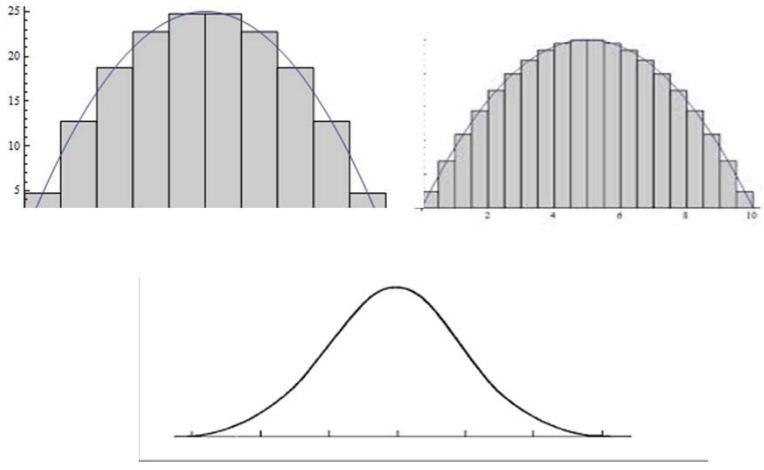

The Innovation Matrix –
Where does the Innovative Lawyer Fit?
Old Tech/Old Apps
Mailing/Faxing Depositions
InPerson Depositions
New Tech/Old Apps
LegalZoom
Docracy
Old Tech/New Apps
?What lawyer has done the equivalent of building the airplane with bicycle parts?
New Tech/New Apps
How does the Next-Gen Lawyer move into this box?
14

Low □High Hanging Fruit



15

From Geometric Representation to Accurate Topology



16

Lawyer value in an AI World: Working in the Gray Area

Lawyers should learn from Internet Ventures: Do what you do best -- link to the rest.

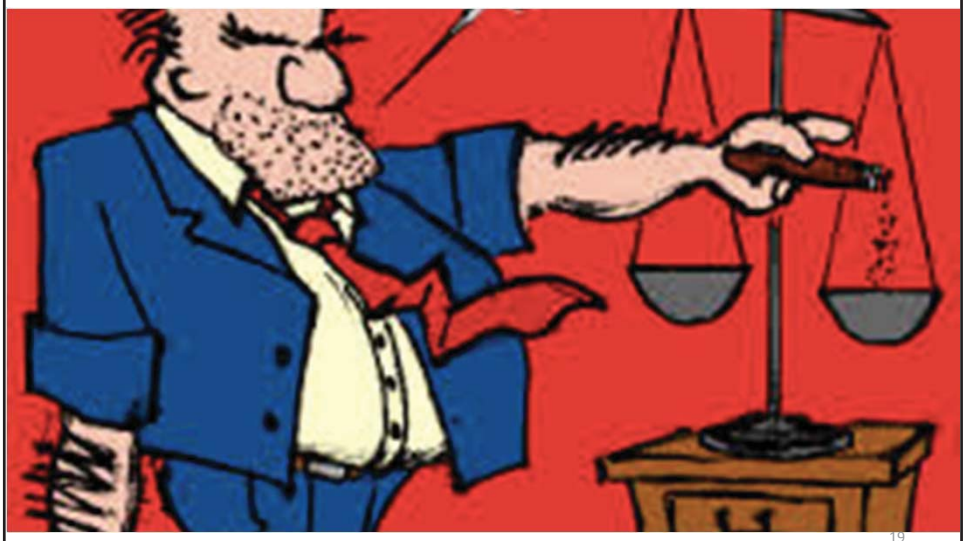
17

Legal Automation and Rudimentary AI

- GDPR:
  - Learning Tool: https://potkewitz.github.io/QnA/GDPR_Learner.html
  - Letter Tool: https://potkewitz.github.io/QnA/GDPR_Letter.html
- FOIAs, expungements, takedowns

18

Current Generation of Lawyer Ill-Equipped
But is AI Better Equipped?

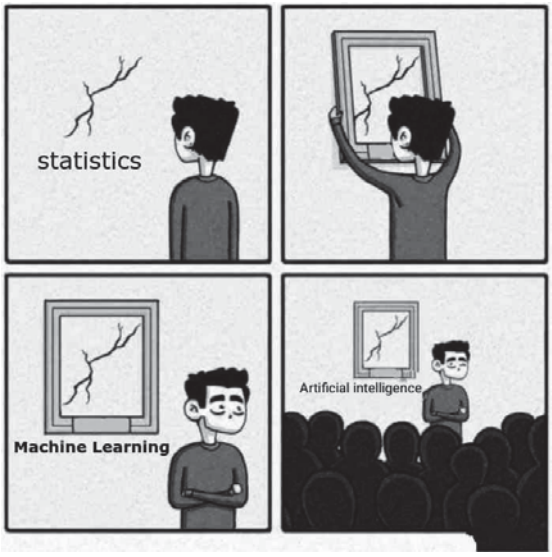


19

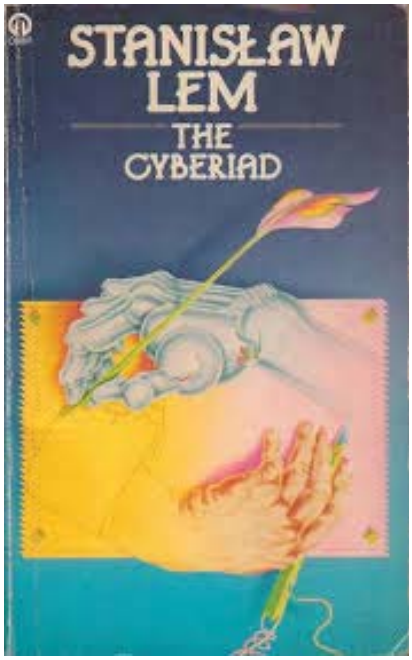
Human/Bot battles and/or collaborations
AI as fact-finder / Lawyer as ethicist

20

AI as Creator



21

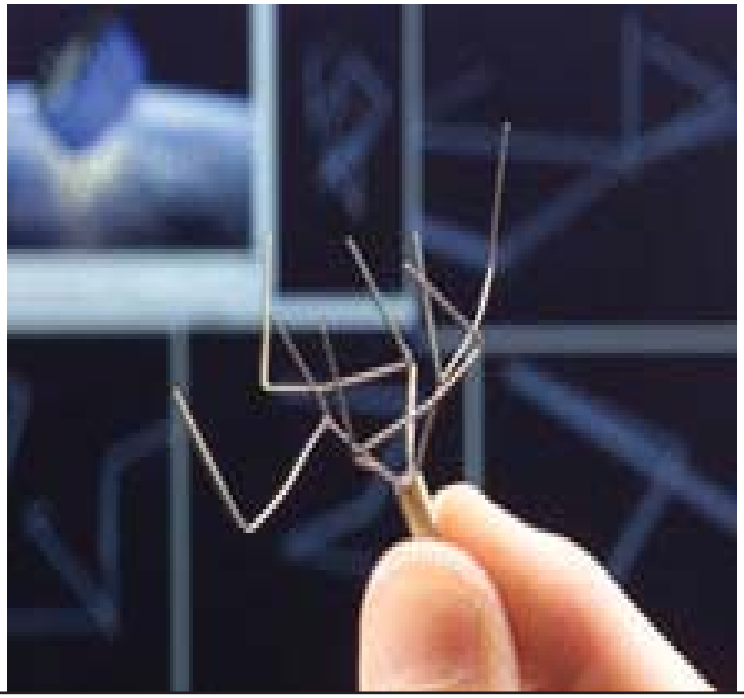


22

Remember when the IP Implications of 3D Printing seemed Profound?

23

24




Oral-B

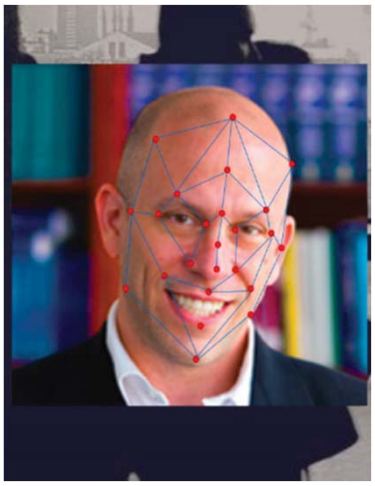

UPDATE
GOOGLE A.I. JUST CREATED A SONG

27


DEVELOPING STORY
SELFIE DISPUTE OVER MONKEY'S VIRAL SNAP
PHOTOGRAPHER SQUARING OFF AGAINST WIKIPEDIA
abc
5:35

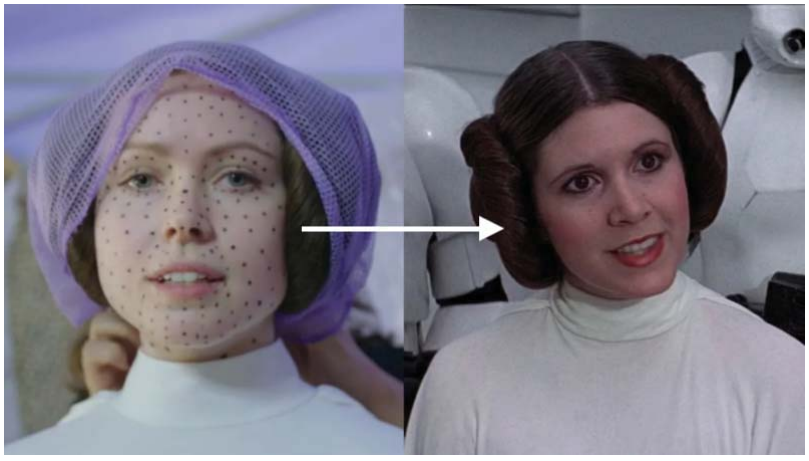
28

AI and Facial Recognition



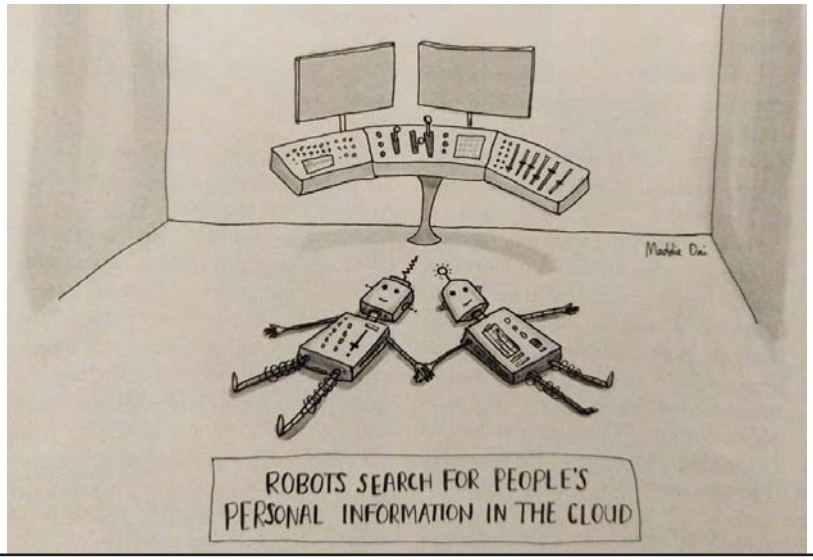
29

AI and Deepfakes



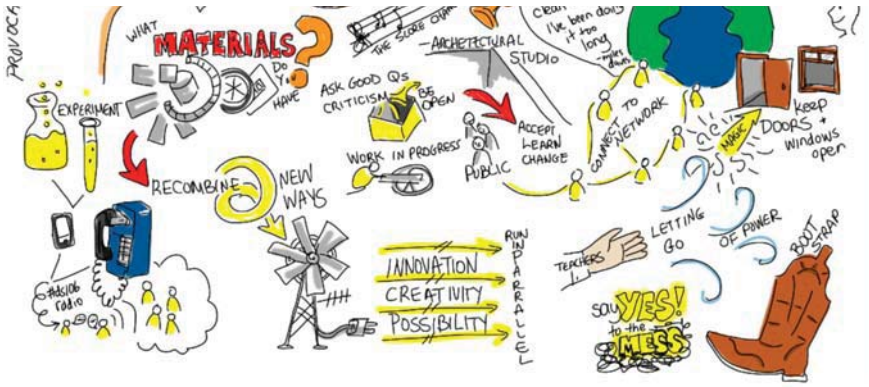
30

Legal testbeds and infinite legal simulators



31

AI at The Adjacent Possible Party



32

AI and the Law School: Challenges and Innovations
Presented to: New York State Bar IP Section, April 5, 2019

Matthew D'Amore
Associate Dean, Cornell Tech
Professor of the Practice
Cornell Tech
Cornell Law School

1) Innovators have been looking to "artificial intelligence" in law for thirty years.[1]
    a) Early work in expert systems to improve access to the law and to legal decision-making[2]
        i) But note unintended consequences of algorithmic bias and secrecy.[3]
2) Today: An Explosion of Innovation
    a) More than 1100 legal tech startups in the market.[4]
    b) Millions of dollars in funding[5]
    c) Significant acquisition activity[6]
    d) Many law firms developing in-house incubators and innovation laboratories[7]
3) Law schools have been innovating also[8]
    a) Innovation labs to app development to service delivery examples abound
4) How to Teach AI at the Law School Level?
    a) Who is the "consumer"?
    b) What is the goal?

---

[1] See Berman and Hafner, The Potential of Artificial Intelligence to Help Solve the Crisis in our Legal System, Communications of the ACM, 32:8 (Aug. 1989) 928
[2] *Id*.
[3] Michael Veale, Max Van Kleek, and Reuben Binns. 2018. Fairness and Accountability Design Needs for Algorithmic Support in High-Stakes Public Sector Decision-Making. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18). ACM, New York, NY, USA, Paper 440, 14 pages. DOI: https://doi.org/10.1145/3173574.3174014; N. Ram, Innovating Criminal Justice, 112 Nw. U. L. Rev. 659 (2018).
[4] https://techindex.law.stanford.edu/
[5] https://blog.lawgeex.com/3-charts-that-show-the-unstoppable-growth-of-legal-tech/
[6] Id.
[7] R. Strom, Build or Buy? Orrick to Do Both as Firm Plans to Invest in Legal Tech Startups, The American Lawyer, Nov. 15, 2018. https://www.law.com/americanlawyer/2018/11/15/build-or-buy-orrick-to-do-both-as-firm-plans-to-invest-in-legal-tech-startups/
[8] Z. Warren, You Think Legal Education Can't Change? 8 Innovative Ideas from Law Schools, Legaltech News, Nov. 20, 2018. https://www.law.com/legaltechnews/2018/11/20/you-think-legal-education-cant-change-8-innovative-ideas-from-law-schools/

c) How to teach legal tech / AI alongside the rule against perpetuities?

5) Who is the consumer?

a) Law students?[9]

i) Law students choose among a market of competing law schools; is tech a consideration?

ii) Want thought-provoking deep learning opportunities (aka "tech is cool")

(1) Some portion will enter legal academia or policy making roles in these areas (e.g., NGOs, FCC, FTC, FDA; also corresponding international bodies)[10]

iii) Want work as a lawyer

(1) Different firms and practices have different needs (see below)

iv) May want non legal tech-centric jobs

(1) E.g. legal tech or e-discovery[11]

b) Law firms?

i) Law students compete for attorney jobs; is AI knowledge or experience needed?

ii) Large law firm tech needs: knowledge management, e-discovery/due diligence, data management, expert systems, document creation/automation (plus client management – e.g., billing, timekeeping, etc.)

iii) Small law firm tech needs: automation/workflow, document creation/automation, intake, client/matter management tools; and maybe all of the above.

iv) Both large and small firms serving technology companies need attorneys who can speak "client"

v) Same questions arise: Do we want lawyers who "know" AI or "use" AI, and how are they valued in the market?

c) Legal Tech companies?

i) Legal industry knowledge, practice experience, thought leadership, product and business development skills, design skills, product management, sales

---

[9]See generally A. Bottner, Law Technology Today, April 13, 2016. https://www.lawtechnologytoday.org/2016/04/know-youll-study-law-school-next-semester/

[10] See, e.g., A. Tutt, An FDA for Algorithms, 69 Admin. L. Rev. 83 (2017)

[11] G. Simons, Hack Your Way to a Job in Legal Technology, Lawyerist, Nov. 16, 2018 https://lawyerist.com/hack-legal-tech-job/; K. Twigger, The Crucial Role Of The Project Manager In eDiscovery, Above the Law, Sept. 12, 2017. https://abovethelaw.com/2017/09/the-crucial-role-of-the-project-manager-in-ediscovery/

d) New service delivery models[12]

i) E.g., Legal Process Outsourcing and Alternative Legal Service Providers

6) Teaching the Law of AI

a) Closest to traditional law teaching (but maybe a little more fun)

b) Key issues

i) Regulation of autonomous devices

ii) Bias in AI decision making (esp. when used for judicial / legal procedures)

iii) "Causation Challenge" - tort law issues

iv) Privacy / big data

c) Examples: Law of AI and AI regulation

i) University of Pittsburgh Law School: Artificial Intelligence and Legal Reasoning Seminar[13]

ii) Stanford Law School: Regulating Artificial Intelligence[14]

iii) Columbia Law School: Technology, Business, Law and Policy of AI[15]

iv) Cornell Law School / Cornell Tech: Law of Robots[16]

v) Vanderbilt Law School: Robots, Artificial Intelligence and the Law[17]

d) Big Data approaches

i) Hofstra School of Law: Law, Logic and Technology Research Laboratory[18]

7) Use of AI / Legal Tech for the Practice of Law

a) Lexis / Westlaw taught in law school for decades

i) Legal tech as legal research

ii) Give away the razors, sell the blades

[12] S. Caserta and M. Madsen, The Legal Profession in the Era of Digital Capitalism: Disruption or New Dawn?, Laws 2019, 8(1), 1; https://doi.org/10.3390/laws8010001
[13] https://www.law.pitt.edu/academics/courses/catalog/5895
[14] https://law.stanford.edu/courses/regulating-artificial-intelligence/
[15] https://www.law.columbia.edu/courses/sections/24578
[16] https://classes.cornell.edu/browse/roster/SP19/class/LAW/6643
[17] https://law.vanderbilt.edu/courses/409
[18] https://law.hofstra.edu/facultyandresearch/centers/lltlab/

b) E-discovery programs

i) Responding to litigation demand for eDiscovery

c) Examples:

i) Vermont Law School: ELawyering and Big Data[19]

ii) Vanderbilt Law School: Electronic Discovery and Information Governance[20]

iii) Cleveland-Marshall College of Law EDiscovery Professional Certificate[21]

iv) Duke Law: Writing Seminar: Electronic Discovery[22]

v) Chicago-Kent School of Law: legal tech as legal research and training[23]

8) The University of Oklahoma College of Law Model[24]

a) Understand the target market: small law firms

b) Focus on software / AI utilization

c) Build curriculum around utilization

9) Hybrid Models

a) UC Hastings:[25]

i) Using Artificial Intelligence in Legal Practice

ii) Legal Tech Startup Skills

b) Cornell Law School / Cornell Tech Master of Laws in Law, Technology and Entrepreneurship[26]

c) Duke Center on Law and Technology[27]

d) Brooklyn Law Incubator & Policy Clinic[28]

10) Law schools as incubators for legal tech and access to justice innovation

---

[19] https://www.vermontlaw.edu/academics/courses/business-law/bus6361
[20] https://law.vanderbilt.edu/courses/304
[21] https://www.law.csuohio.edu/programs/certificates/ediscovery
[22] https://law.duke.edu/academics/course/787/
[23] S. Ward, There's a variety of affordable—or free—ways to teach legal tech, law school librarians say, ABA Journal, March 1, 2019. http://www.abajournal.com/news/article/theres-a-variety-of-affordable-or-free-ways-to-teach-legal-tech-say-law-school-librarians/
[24] https://law.ou.edu/news-and-media/ou-college-law-launches-center-technology-and-innovation-practice
[25] UC Hastings Law to Add AI, Startup Tech Courses, Law Technology News, Nov. 21, 2017.
[26] https://tech.cornell.edu/programs/masters-programs/master-of-laws-llm/
[27] https://law.duke.edu/dclt/
[28] https://www.brooklaw.edu/academics/clinicalprogram/blip/aboutblip?

a) App Development, Expert Systems and Self Help

i) Cornell Law School / Cornell Tech: Delivering Legal Services Through Technology[29]

ii) Cornell Law School Technology, Innovation and the Law Clinic[30]

iii) Cornell Law School Legal Information Institute[31]

iv) Columbia Law School Lawyering in the Digital Age Clinic[32]

v) Chicago Kent College of Law Center for Access to Justice & Technology[33]

vi) Stanford Law School: Legal Design Lab[34]

b) Data driven approaches

i) Access to Justice Lab at Harvard Law School[35]

ii) National Center for Access to Justice at Fordham Law School[36]

11) How to Teach AI at the Law School Level?

a) No single approach is right:

i) Law schools need to follow their market

(1) Will differ for each law school

(2) Will evolve as each market changes

ii) Will need to adapt more quickly to changing legal technology and legal practice models

b) Public / private partnerships may be important

i) Westlaw, Lexis, UnitedLex, Neota

[29] http://news.cornell.edu/stories/2018/12/law-business-students-develop-ai-apps-aid-nonprofits
[30] https://www.lawschool.cornell.edu/spotlights/immigration-innovation-challenge.cfm
[31] https://www.law.cornell.edu/
[32] https://www.law.columbia.edu/clinics/lawyering-in-the-digital-age-clinic
[33] https://www.kentlaw.iit.edu/institutes-centers/center-for-access-to-justice-and-technology
[34] https://law.stanford.edu/organizations/pages/legal-design-lab/
[35] https://a2jlab.org/
[36] https://ncforaj.org/

AI and the Law School: Challenges and Innovations

Matthew D'Amore
Associate Dean, Cornell Tech
Professor of the Practice
Cornell Tech
Cornell Law School

NEW YORK STATE BAR ASSOCIATION
LAWYERING IN THE AGE OF BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE

Cornell Law School

JACOBS INSTITUTE AT CORNELL TECH

SPECIAL SECTION

Social Aspects of Computing

Rob Kling Editor

The Potential of Artificial Intelligence to Help Solve the Crisis in Our Legal System

Donald H. Berman and Carole D. Hafner

Cornell Law School

JACOBS INSTITUTE AT CORNELL TECH

SPECIAL SECTION

Social Aspects of Computing

Rob Kling Editor

The Potential of Artificial Intelligence to Help Solve the Crisis in Our Legal System

Donald H. Berman and Carole D. Hafner

928 *Communications of the ACM* August 1989 Volume 32 Number 8

Cornell Law School

JACOBS INSTITUTE CORNELL TECH

AI & the Law School: Matthew D'Amore

Today: An Explosion of Innovation

https://blog.lawgeex.com/3-charts-that-show-the-unstoppable-growth-of-legal-tech/legal-ai-landscape-lgeex/

Cornell Law School

JACOBS INSTITUTE CORNELL TECH

Today: An Explosion of Innovation

https://abovethelaw.com/law2020/directory-of-law-school-innovators/

AI & the Law School: Matthew D'Amore

How to Teach AI at the Law School Level?

- Several approaches:
  - Law of AI
  - Use of AI / Legal Tech
  - Development of AI / Legal Tech
  - Access to Justice (A2J)
  - Hybrid Models

http://technosiren.com/amm/wp-content/uploads/sites/18/2015/03/throwing-spaghetti.jpg

Considerations and Context

- Who is the "consumer"?
- What is the goal?
- How is legal tech / AI used in practice?
- How to teach legal tech / AI alongside the rule against perpetuities?

Who is the consumer?

- Law students?
  - Want thought-provoking deep learning opportunities
  - Find AI exciting and cutting edge ("Law of Robots")
  - Want legal jobs
  - May want non legal jobs
- Law firms?
  - Big vs. small vs. solo
- In-house legal departments?
- Legal Tech companies?

What is the goal?

PRACTICE OF LAW FOR AI CLIENTS

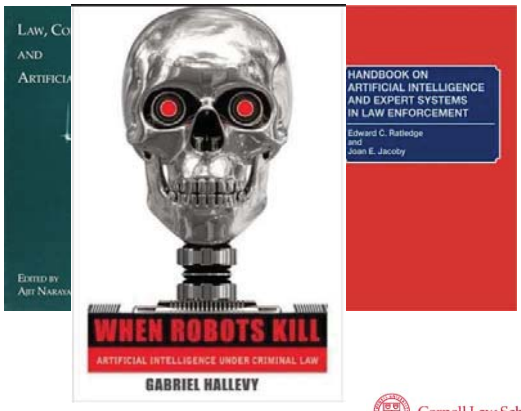
USE AI FOR THE PRACTICE OF LAW

LEGAL TECH INNOVATION

AI & the Law School: Matthew D'Amore

Teaching the Law of AI

- Closest to traditional law teaching (but maybe a little more fun)



Cornell Law School

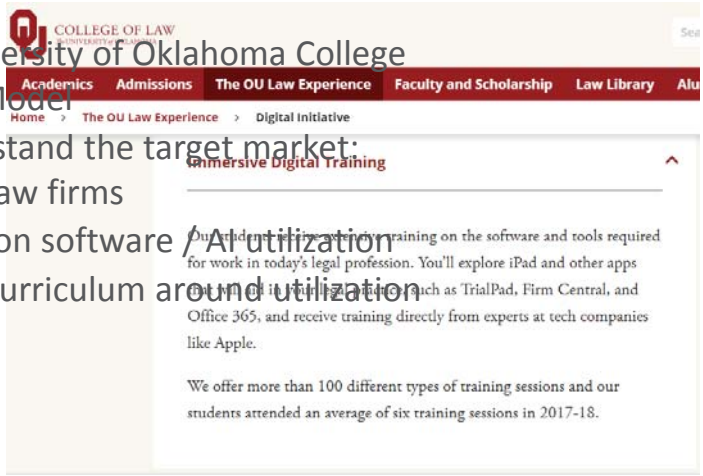
JACOBS INSTITUTE
CORNELL TECH

Teaching the law of AI

- Key issues
  - Regulation of autonomous devices
  - Bias in AI decisionmaking (esp. when used for judicial / legal procedures)
  - "Causation Challenge" - tort law issues
  - Privacy / big data
    - Data needed to build the AI tool in the first place
  - Clinics to deliver legal services to startups in the field (Brooklyn Law)

Use of AI / Legal Tech for the Practice of Law

- The University of Oklahoma College of Law Model
  - Understand the target market: small law firms
  - Focus on software / AI utilization
  - Build curriculum around utilization



AI & the Law School: Matthew D'Amore

Use of AI / Legal Tech for the Practice of Law

MAY 28, 2015

Legaltech© news ONLINE

An ALM Publication

FOUR U.S. LAW SCHOOLS AND UNITEDLEX LAUNCH LEGAL RESIDENCY PROGRAM

Emory University School of Law, the University of Miami School of Law, The Ohio State University Moritz College of Law and Vanderbilt Law School participate in first-ever legal residency program.

Cornell Law School

JACOBS INSTITUTE CORNELL TECH

AI & the Law School: Matthew D'Amore

Legal Tech Innovation

HOFSTRA | LAW

LAW, LOGIC & TECHNOLOGY RESEARCH LABORATORY

The Research Laboratory for Law, Logic and Technology (LLT Lab) conducts empirical research on argument and reasoning patterns in diverse samples of legal documents, creating the semantic data, training protocols, and software analytics needed to develop technology to assist legal reasoning.

DUKE LAW TECH LAB

What We Do

We accelerate the next generation of startups that will change the way legal and civic services are delivered

SLS THE LEGAL DESIGN LAB

The Legal Design Lab is an interdisciplinary team based at Stanford Law School & d.school, building a new generation of legal products & services.

JACOBS INSTITUTE AT CORNELL TECH

Cornell Law School

NEOTA LOGIC

IMPACT

Runway Startups

Legal Tech Innovation

Cornell Law School

NEOTA LOGIC

JACOBS INSTITUTE AT CORNELL TECH

IMPACT Runway Startups

AI & the Law School: Matthew D'Amore

Access to Justice

Expert Systems & Selfhelp

Columbia Law School

Lawyering in the Digital Age Clinic

Chicago-Kent College of Law
ILLINOIS INSTITUTE OF TECHNOLOGY

Center for Access to Justice & Technology

Cornell Law School

LAW 7960 - Technology, Innovation and the Law Clinic

Data-driven approaches

Welcome to the National Center for Access to Justice at Fordham Law School

Our vision:

The National Center for Access to Justice at Fordham Law School is the national organization using data to accomplish change that assures access to justice. Access to justice — the ability to understand the law and obtain its protection — often makes all the difference for people, enabling families to stay together, to save their homes, to protect themselves from harm, and even to preserve their liberty.

ACCESS TO JUSTICE LAB
AT HARVARD LAW SCHOOL

OUR VISION

Imagine if lawyers, judges, and policymakers used rigorous evidence to design and run the U.S. justice system.

Hybrid Models

UC Hastings Law to Add AI, Startup Tech Courses

"Using Artificial Intelligence in Legal Practice" will help students build familiarity in using AI-based research platforms, while "Legal Tech Startup Skills" will guide students through launching their own companies.

By **Gabrielle Orum Hernández** | November 21, 2017 at 11:30 AM

https://www.law.com/legaltechnews/sites/legaltechnews/2017/11/21/uc-hastings-law-to-add-ai-start-up-tech-courses

JACOBS INSTITUTE CORNELL TECH

Cornell Law School

AI & the Law School: Matthew D'Amore

Hybrid Models

DUKE CENTER ON LAW&TECH

Courses on Law & Technology at Duke Law

- Law of Robots and Exponential Technologies
- Frontier Tech of Legal Practice
- Contract Drafting: The Next Generation
- FinTech and the Law
- eDiscovery
- Introduction to Technology in the Law Office
- Information Privacy and Government Surveillance Law
- Frontier AI & Robotics: Law & Ethics
- The Law and Policy of Innovation: the Life Sciences
- Patent Law and Policy
- Data Breach Response and Cybersecurity Due Diligence
- Trademark Protection and the Changing Landscape of the Internet
- Law & Policy: Blockchain
- Designing Creative Legal Solutions

JACOBS INSTITUTE CORNELL TECH

Cornell Law School

Hybrid Models

CORNELL TECH
HOME OF THE JACOBS INSTITUTE

Cornell Law School

JD Program in Information and Technology Law (Cornell Tech campus)

SELECTED COURSE OFFERINGS INCLUDE:

- Law of Financial Technology
- Internet Law, Privacy, and Security
- Cyber Enforcement, Regulation & Policy Analysis
- Venture Capital
- Free Speech Law on the Internet
- Trade Secrets Law and Practice
- Intellectual Property
- Law of Robots
- Digital Health Law

AI & the Law School: Matthew D'Amore

How to Teach AI at the Law School Level?

http://t
content/upl wing-spaghetti.jpg

x

How to Teach AI at the Law School Level?

- No single approach is right:
  - Law schools need to follow their market
    - Will differ for each law school
    - Will evolve as each market changes
- Public / private partnerships
  - Westlaw, Lexis, UnitedLex, Neota
- Law schools as incubators for legal tech innovation
- Law schools as incubators for access to justice innovation

CONTRACT ANALYTICS – APPLICATION OF AI

I. AN OVERVIEW OF MACHINE LEARNING (ML)

a. What is Artificial Intelligence (AI)?

The term artificial intelligence was coined in 1955 by John McCarthy, a math professor at Dartmouth. Ever since then, the field has given rise to many extravagant claims and promises. At its core, Artificial Intelligence is essentially a machine that can perform tasks thought to require human level intelligence. As a result, AI has as varied applications as the applications of human cognition itself.

To provide some context, let's draw a distinction between Strong AI and Weak AI.

- Strong AI is essentially a machine with a "mind" that is roughly as capable as a human at any task requiring general intelligence.

- Weak AI, also known as "Applied AI," is where AI development in the current world has really focused. Weak AI relates to the use of a purpose-built machine to perform a specific task that has traditionally required a human.

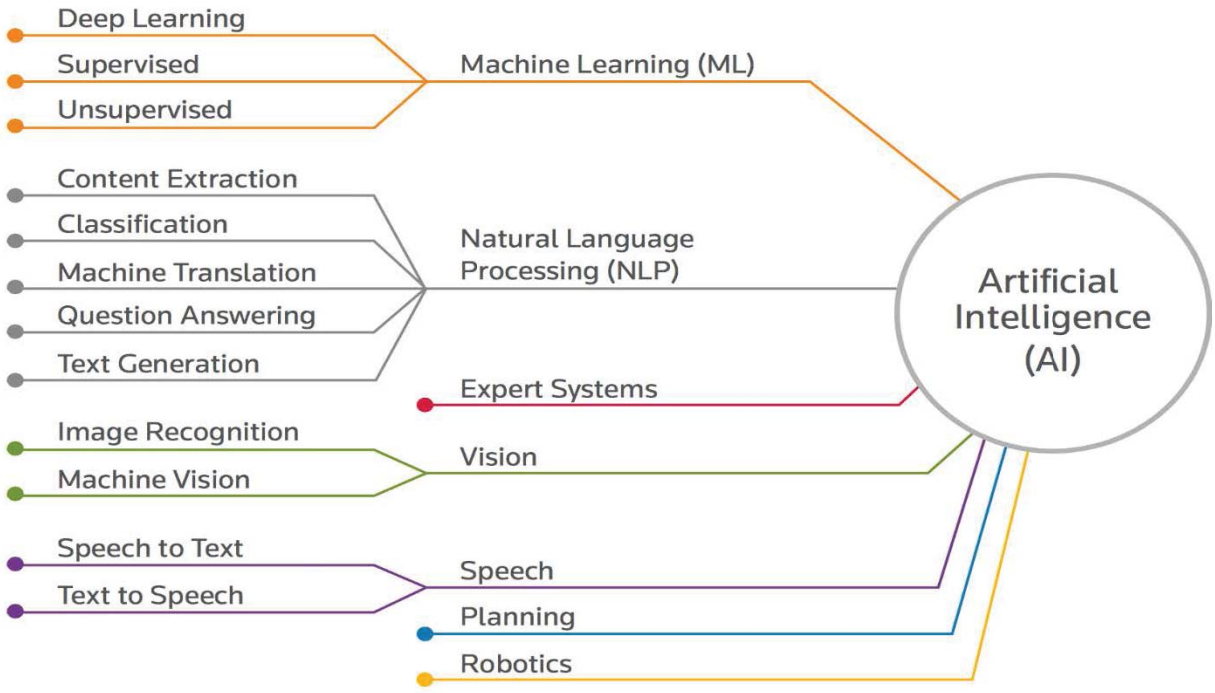
  Weak certainly doesn't mean incapable. Weak AI can: (i) land airplanes in bad weather, (ii) detect insider trading; and (iii) translate between languages.

  The biggest advances to date in weak AI have been in two broad areas of AI: perception and cognition.

  In the former category some of the most practical advances have been made in relation to speech. Voice recognition is still far from perfect, but millions of people are now using it — think Siri, Alexa, and Google Assistant. A study by the Stanford computer scientist James Landay and colleagues found that speech recognition is now about three times as fast, on average, as typing on a cell phone (source: Stanford News, August 24, 2016, https://news.stanford.edu/2016/08/24/stanford-study-speech-recognition-faster-texting/). "The error rate, once 8.5%, has dropped to 4.9%. What's striking is that this substantial improvement has come not over the past 10 years but just since the summer of 2016." (source: "Artificial Intelligence & Machine Learning: Demystified," https://www.cpm-int.com/icc/blog/post/artificial-intelligence-machine-learning-demystified/)

In the latter category of cognition and problem solving, machines have already beaten the finest (human) players of poker and Jeopardy; achievements that experts had predicted would take at least another decade. Intelligent agents are being used by cybersecurity companies such as Deep Instinct to detect malware, and by PayPal to prevent money laundering. Dozens of companies are using this form of weak AI, and specifically machine learning, to decide which trades to execute on Wall Street, and more and more credit decisions are made with its help.

Below are some types of Artificial Intelligence:



(source for diagram: "Artificial Intelligence: Definition, Types, Examples, Technologies, by Chethan Kuman GN, https://becominghuman.ai/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b)

Many of the legal applications that incorporate Artificial Intelligence leverage machine learning and natural language processing.

- Natural language processing or NLP is an area that is a confluence of AI and linguistics. It involves intelligent analysis of written language. It is a field of AI that researches how computers can create, understand or consume human language. If you have a lot of data written in plain text and you want to automatically get some insights from it, you need to use NLP techniques. These insights could be – sentiment analysis, information extraction, information retrieval, search, etc.

- Machine learning is an area of AI that utilizes a set of statistical techniques for problem solving. Machine learning studies programs that can learn concepts or recognize patterns on their own, without being programmed for each task. These techniques can be applied to a wide variety of problems. In order to apply ML techniques to NLP problems, we need to convert the unstructured text into structured format. The most important thing to understand about ML is that it represents a fundamentally different approach to creating software: The machine learns from examples, rather than being explicitly programmed for a particular outcome.

b. <u>How does Machine Learning work?</u>

Here is an example of machine learning in the legal world:

> Imagine you wanted to teach the software to identify Change of Control provisions. You could provide it with examples and the system could memorize the examples. Every time it encountered a new document where the language matched one of the examples it would be able to identify the relevant language as Change of Control with 100% accuracy.
>
> However, we all know that in the real world, legal concepts can be expressed in a wide variety of ways. Change of Control could be expressed using language like "assignment by operation of law" or "sale of all or substantially all of a company's assets." We wouldn't want to miss these because the software had not seen the exact wording before.

Let us contrast this to how humans work:

> Human's may discover some simple rules of thumb which helps to guide their analysis. For example, if 'Change' appears within 3 words of 'Control' the provision is likely Change of Control **OR "**assignment by operation of law" is a synonym of "change of control".

With machine learning, the system reviews numerous examples of a concept. It tries millions of different rules and keeps those with predictive power. It's then able to make predictions on new documents that it hasn't seen before.

This will not achieve 100% accuracy, but can perform at 90% or more on never-before-seen documents.

To think about it another way we could use two examples that were cited in a recent article in Business Law Today called "A Simple Guide to Machine Learning" written by Warren E. Agin. To wit, humans are good at deductive reasoning.

- Example 1: If someone were to tell you that a bankruptcy claim for rent was limited to one year's rent, you would easily figure out the amount of the allowed claim. If the total rent claim were $100,000, but one year's rent was $70,000, you would apply the rule and deduce that the allowable claim is $70,000. Now reverse the process. Assume you were told that your client was owed $100,000 and that the annual rent was $70,000, and then told you that the allowable claim was $70,000. Could you determine how that answer was obtained? You might guess that the rule is that the claim is limited to one year's rent, but could you be sure? Perhaps the rule was something entirely different. This is inductive reasoning, and it is much more difficult to do. (source: "A Simply Guide to Machine Learning" by Warren E. Agin, Business Law Today, February 2017, https://www.americanbar.org/content/dam/aba/publications/blt/2017/02/machine-learning-201702.pdf)
- Example 2: Think about a series of numbers: 2, 4, 6, 8, 10 and you're asked to identify the next number. Here we induce a rule that you add 2 to each number in the series and determine that the next number would be 12. (source: "A Simply Guide to Machine Learning" by Warren E. Agin, Business Law Today, February 2017, https://www.americanbar.org/content/dam/aba/publications/blt/2017/02/machine-learning-201702.pdf)

Machine learning techniques are computational methods for figuring out "the rules," or at least approximations of the rules, given the factual inputs and the results. Those rules can then be applied to new sets of factual inputs to deduce results in new cases. In a more complicated setting to build a prediction model, contract analytics would be utilized by having attorneys annotate language and then create a training set and a test set. Then we would begin to analyze the various relationships among the data points in our training set using statistical methods. Statistical analytics can help us identify the factors that seem to correlate with the known results and the factors that clearly do not matter.

c. <u>AI in Knowledge Work</u>

Bank of America Merrill Lynch predicts that AI will have a $9 trillion dollars impact on knowledge work by 2025. The McKinsey Global Institute says AI is driving transformation of society at a rate of "3,000 times the impact" of the Industrial Revolution. (source: "The return of the machinery question" The Economist, June 25, 2016, https://www.economist.com/special-report/2016/06/25/the-return-of-the-machinery-question)

A widely cited study by Carl Benedikt Frey and Michael Osborne of Oxford University, published in 2013, found that 47% of jobs in America would be impacted by "computer capital". (source: "The Future of Employment: How

Susceptible Are Jobs to Computerisation?" by Carl Benedikt Frey and Michael A. Osborne, September 17, 2013, https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf)

d. Applications of ML

There are a variety of ways in which AI is being leveraged in the legal profession. These include:

- eDiscovery
- Litigation Analysis and Outcome Prediction which identify which courts are more likely to render favorable verdicts.
- Legal Research
- Intellectual Property Law
- Contract Review and Due Diligence

II. CONTRACT ANALYTICS

Before we get in to AI-based contract analytics specifically, let us consider the traditional approach to large scale contract review. This is less about reviewing drafts of one-off contracts that you're in the midst of negotiating and more about reviewing a large volume of contracts such as when conducting due diligence in M&A or going through your company's customer contracts to track certain data points or to ensure compliance with the new revenue recognition accounting standards.

Attorneys or other reviewers will typically read through the contracts looking for key data. They'll then summarize the contract by copying & pasting key data into Excel, Word or a Contract Management System. Abstracts and summaries go through multi-step quality control review. The process can take weeks or months. It is typically slow, expensive and error-prone.

Contract Analytics, on the other hand, deploys machine learning and natural language processing technology. This type of software is able to extract legal concepts regardless of the specific vocabulary used or the location of the concept in the document. In other words, as we discussed earlier, the software is trained to extract a concept like Change of Control whether it is described using the phrase "Change of Control", "assignment by operation of law" or "sale of all or substantially all of a company's assets." It is also designed to identify this concept whether it is in a standalone Change of Control section or buried somewhere in a Termination section. Some contract analytics systems also allow users to train the software themselves to extract custom terms to meet their specific needs.

The main reasons corporations and law firms will leverage contract analytics is for time savings, cost savings and accuracy improvements.

- Time savings are variable and depend on the complexity of the project and experience of the reviewer. In many situations they are significant.
- From a corporate legal department standpoint, time savings translates into cost savings. Many of the junior attorneys performing due diligence at outside law firms for example are billed out at hundreds of dollars per hour.
- Improvements in accuracy is really the third part of the value proposition associated with leveraging this type of software. This is not so much a situation where it is measured by human against machine but really more an attorney using the software against an attorney without the software. In a due diligence setting, it is often 1st and 2nd year associates going through complex documents at 2 am which makes it easy for things to fall through the cracks. Leveraging contract analytics tools can help to prevent this from happening.

The following are some typical contract analytics use cases.

a. <u>M&A and other Transactional Uses (Buy & Sell side in M&A)</u>

Machine learning can be leveraged on both the buy side and sell side for transactional work.

On the buy side, it can be used to go through the target companies contracts to summarize their content and identify problematic provisions.

On the sell side, it can also be used to review the company's contracts and populate the disclosure schedules to the merger agreement, stock purchase agreement or asset purchase agreement.

We're seeing increasing numbers of cases where corporations are the licensee of contract analytics software but it is their outside counsel that is primarily using it on their behalf.

b. <u>Contract and Knowledge Management; Vendor and Customer Management</u>

Corporate legal departments use contract analytics to extract information from current and legacy contracts to reduce risk of non-compliance or missing key contractual data and commitments.

In many cases, because they don't have insight into their contracts, companies are paying for things they no longer use or missing out on revenue opportunities.

Contract analytics are used by companies to gain insights into relationships with customers, vendors and partners. We also see companies using contract analytics to assist with complying with the new accounting standards related to revenue recognition and leases.

Because some contract analytics tools allow users to train the system themselves, non-technical users are leveraging their own domain expertise to teach the systems to assist in addressing their own specific pain points as well.

c. Commercial Real Estate and other Leases – Lease Abstraction

Contract analytics can also be used to extract data from company leases. For example, real estate companies are using contract analytics tools to look through their contracts for terms like expiration dates, rent payments, etc. We are also seeing REITs and companies that advise REITs using contract analytics to ensure compliance with REIT regulations and monitoring.

d. Audit & Compliance

- The ASC 606/IFRS 15 Revenue Recognition Standard(s), Revenue From Contracts With Customers, provides accounting guidance related to revenue from contracts with customers. The core principle behind ASC 606 is that an entity recognizes revenue to depict the transfer of promised goods or services to customers in an amount that reflects the consideration to which the entity expects to be entitled in exchange for those goods or services. Following this core principle, an entity recognizes revenue by applying the following steps:

  Step 1: Identify the contract(s) with a customer
  Step 2: Identify the performance obligations in the contract
  Step 3: Determine the transaction price
  Step 4: Allocate the transaction price to the performance obligations in the contract
  Step 5: Recognize revenue when (or as) the entity satisfies a performance obligation

  Contract Analytics has immediate overlap in assisting entities and their audit/accounting firms in identifying the performance obligations in a contract (Step 2) and determining the transaction price (Step 3).

- Corporations looking to understand their financial position from the company's contracts use auditors to review and analyze a large sample set of documents.

  Contract analytics helps auditors to analyze contracts and extract relevant audit data. Reviewers are able to review contracts significantly more efficiently and auditors can review larger sample sets within time and budget constraints. This decreases the audit risk of certifying a company's financial statements.

e. Future of Contract Analytics

We're really just at the threshold of what artificial intelligence can do in the context of contract review and within the legal industry generally.

We'll continue to see contract analytics move out horizontally as it gets into new contract specific domains.

We'll also see it move vertically up the value chain as well. Currently, most contract analytics systems are primarily focused on extracting data from contracts. As AI continues to evolve, these systems will take an increased role in analyzing text as well.

Bibliography and other Reading Material

Bibliography:

https://news.stanford.edu/2016/08/24/stanford-study-speech-recognition-faster-texting/

https://www.cpm-int.com/icc/blog/post/artificial-intelligence-machine-learning-demystified/

https://becominghuman.ai/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b

https://www.americanbar.org/content/dam/aba/publications/blt/2017/02/machine-learning-201702.pdf

https://www.economist.com/special-report/2016/06/25/the-return-of-the-machinery-question

https://www.oxfordmartin.ox.ac.uk/downloads/academic/The_Future_of_Employment.pdf

Further Reading Material:

https://hbr.org/2018/02/how-ai-is-changing-contracts

https://www.forbes.com/sites/bernardmarr/2016/09/30/what-are-the-top-10-use-cases-for-machine-learning-and-ai/#b99d12594c90

https://www.forbes.com/sites/forbeslacouncil/2018/07/17/artificial-intelligence-and-the-evolution-of-law/#428a9acf36ee

Contract Analytics
Application of AI
NYSBA CLE Presentation – 4/5/19

Ned Gannon, President, eBrevia, Inc.

eBREVIA
AI-powered document analysis

DFIN

1

Agenda

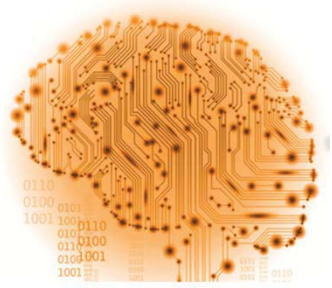
1. AI in the legal industry
2. Why now?
3. Benefits & limitations
4. Contract Analytics
5. Use cases

AI in legal

- eDiscovery
- Litigation Analysis and Outcome Prediction
- Legal Research
- Intellectual Property Law
- Contract Review and Due Diligence
- 606 and 842 Compliance

Artificial Intelligence

Very simply, an Artificial Intelligence is a machine that can perform tasks thought to require human level intelligence. Its applications are as varied as the applications of human cognition.



What is AI: Strong vs. Weak AI

Strong AI

A machine with a "mind" that is roughly as capable as a human at any task requiring general intelligence.

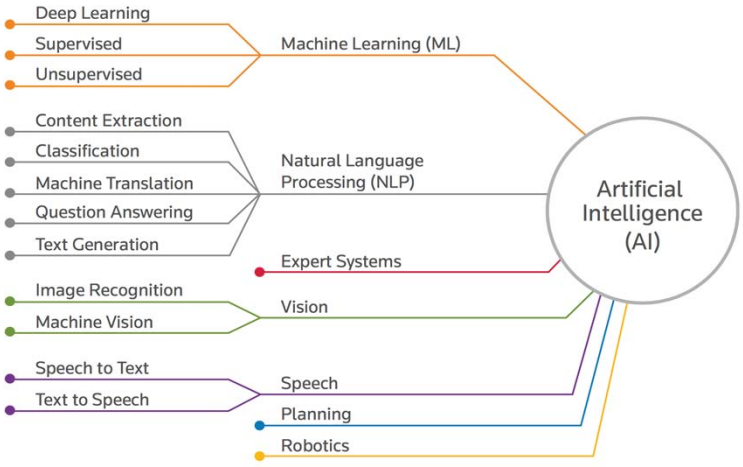
Weak AI

Also "Applied AI". Use of a purpose-built machine to perform a specific cognitive task that has traditionally required a human.

Weak doesn't mean incapable. Weak AIs can:

- Drive cars and land airplanes in bad weather
- Recognize faces
- Read documents
- Detect insider trading
- Translate between languages

Artificial Intelligence



Learning to identify a cat

How does ML work (2 minute version)

...in the event of

a Change in Control

an assignment by operation of law

a sale of all or substantially all of Party B's assets

Party A shall have the right to...

100% accuracy

How does ML work (2 minute version)

...in the event of

a Change in Control

~~an assignment by operation of law~~

~~a sale of all or substantially all of Party B's assets~~

Party A shall have the right to...

100% accuracy

But only on clauses that match what we have seen exactly.

How does ML work (2 minute version)

How do humans work? A human may discover some simple rules:

If 'Change' appears within 3 words of 'Control' the provision is likely Change of Contr

"assignment by operation of law" is a synonym of "change of control".

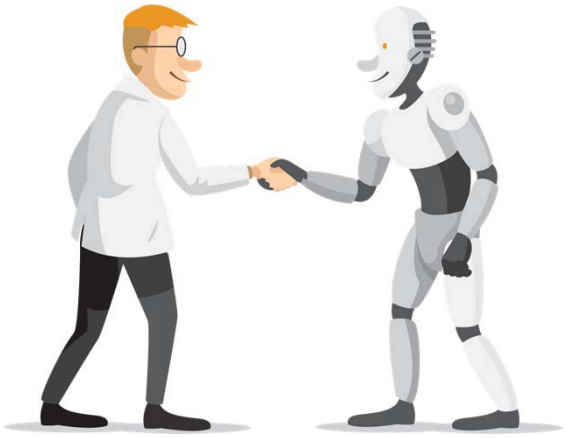
How does ML work (2 minute version)

Will not achieve 100% accuracy, but can perform at 90% or more on never-before-seen documents.

AI in Knowledge Work

> **"The technological breakthroughs of recent years — allowing machines to mimic the human mind — are enabling machines to do knowledge jobs and service jobs…"**
>
> *– New York Times, 12/15/14*

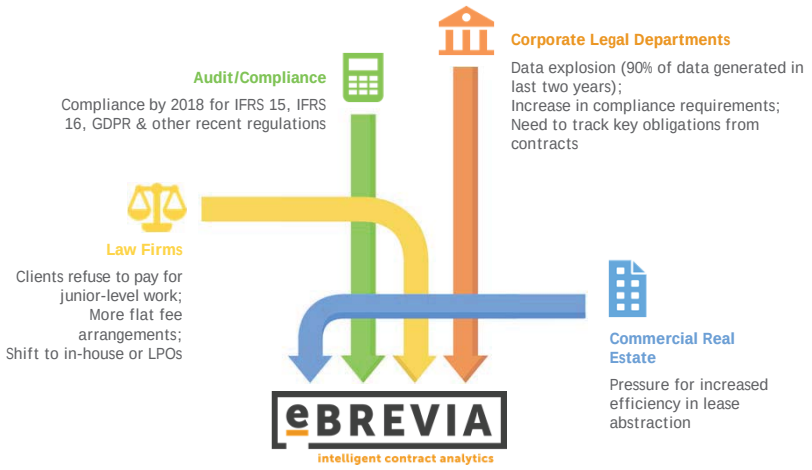
Meet your new associate?



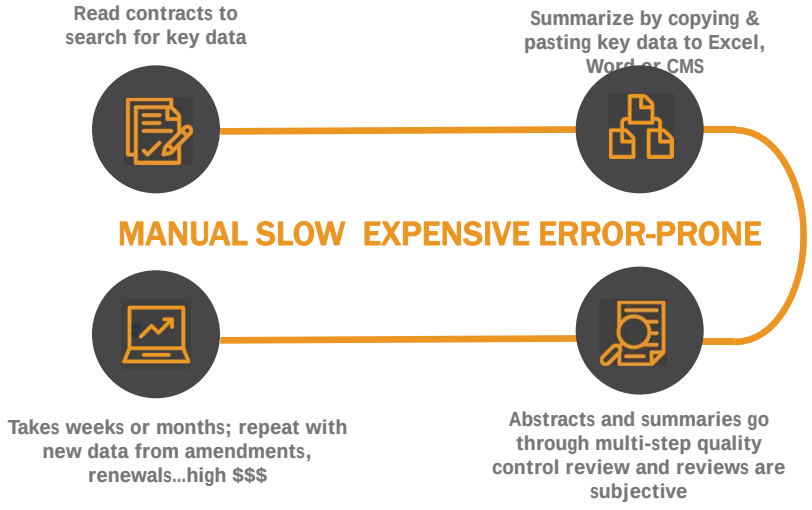
What type of work?

Best fit is routine repetitive work

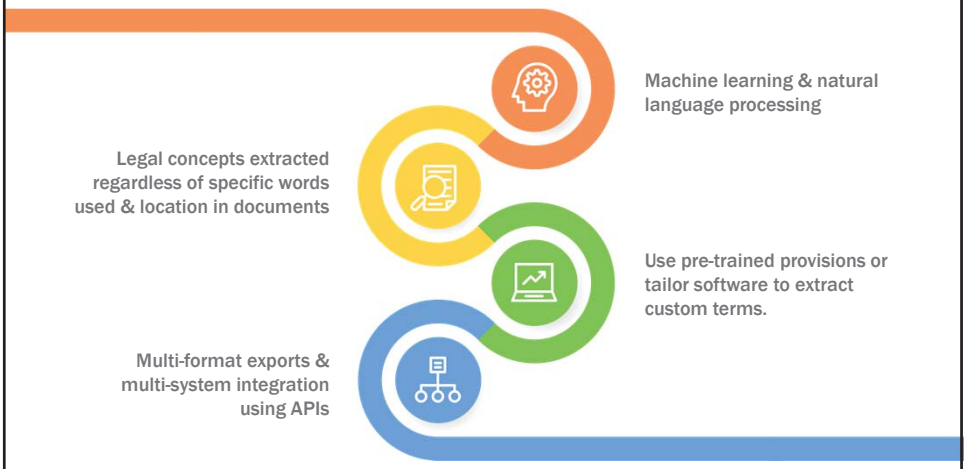
Why now?



Contract Review: Traditional Approach



Contract Analytics



Quantifying ROI

Time savings

Cost savings

Accuracy Improvements

Effects on Business Models

- Alternative fee arrangements
- Rethink pyramid structure
- Segmenting legal work
- Non-traditional services providers
- Enhanced coordination between corporates and outside service providers

Use Cases

Contract Management & Digitization

M&A & Other Transactional Diligence

Audit & Compliance

Vendor & Customer Management

Real Estate & Other Leases

IP Procurement & Management

Human Resources

Bespoke

M&A Due Diligence

Junior Attorneys

Senior Attorneys

Junior attorneys bill **$300-$500/hour** to manually review thousands of contracts to identify and summarize obligations, liabilities, and red flags.

Contract Management

Used to extract information from current and legacy contracts to reduce risk of non-compliance or missing key contractual data and commitments.

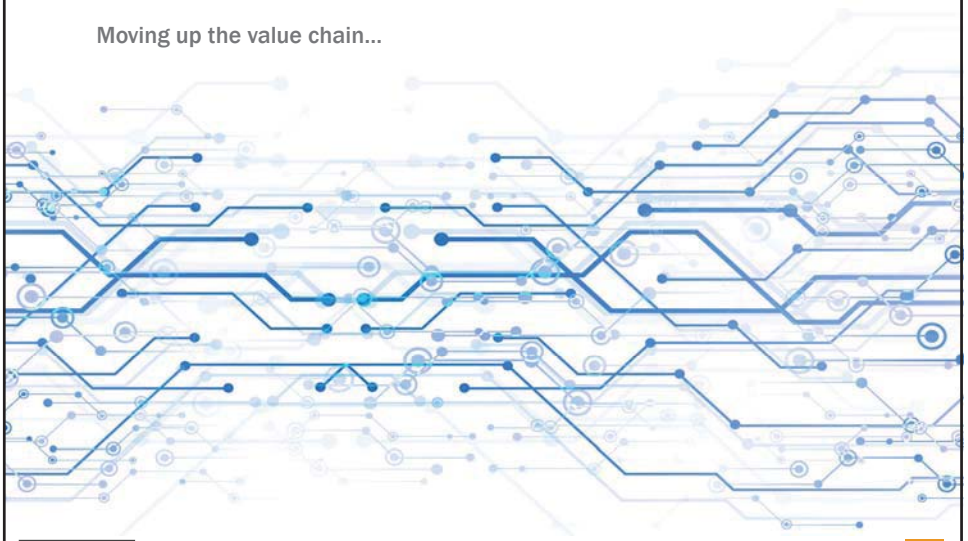
Used to gain insights into relationships with customers, vendors and partners.

Implementation

- Pilots
- Cloud vs. On-premise
- Defining Objectives & Measuring Results
- Project Management
- Training
- Internal Experts
- Resources
- Integrations

The Future of Contract Analytics

Moving up the value chain…



Questions?

NED GANNON

ngannon@ebrevia.com

+1 (203) 870-3000

Speaker Biographies

JONATHAN ASKIN

Biography

Professor Askin is the Founder/Director of the Brooklyn Law Incubator & Policy Clinic (BLIP) and the *Innovation Catalyst* for the Center for Urban Business Entrepreneurship (CUBE). He founded the BLIP Clinic when he joined Brooklyn Law School in 2008, bringing more than a decade of experience in the communications industry from both the public and private sectors. He has provided legal and policy counsel and strategic advice for companies that build and develop communications networks and Internet applications, as well as for other technology-oriented enterprises and startups.

Professor Askin is also Visiting Professor at the Centre for Commercial Law Studies, Queen Mary University of London; a Fellow at the Columbia Institute for Tele-Information; Adjunct Professor at Columbia Law School; and Founder and Advisor to iLINC, a network of legal support clinics for the European startup community.

A sought-after expert in the field of Internet law, he played a key role in the tech task force of President Barack Obama's 2008 election campaign. He has also served as president and general counsel for the Association for Local Telecommunications Services and was a senior attorney at the Federal Communications Commission. He is actively involved in developing Brooklyn as the 21st century "Silicon Alley," recognizing the borough as a burgeoning hub for innovative start-ups, and is affiliated with the Dennis J. Block Center for the Study of International Business Law.

He has served as a board member to many industry groups, including the Universal Service Administrative Company, the North American Numbering Counsel, and the New York Chapter of the Internet Society, and has served as Chair of the Voice on the Net Coalition, as executive director of the Video on the Net Alliance, as president and founder of the Global IP Alliance, and as inaugural Chair of the CyberSpace Committee of the Federal Communications Bar Association. He is a frequent commenter in the media about Internet, communications, and technology-related issues.

At Rutgers Law School he was Notes and Comments Editor for the *Rutgers Law Review*. After law school, he clerked for Chief Justice Robert N. Wilentz of the New Jersey Supreme Court and practiced as an associate at Davis Polk & Wardwell and as a Deputy Public Advocate for the State of New Jersey.

Professor Askin was also a Visiting Professor at the MIT Media Lab and a Fulbright Scholar at the University of Amsterdam's Institute for Information Law.

WILLIAM BELMONT, ESQ.

Biography

As an investigative attorney, Mr. Belmont is experienced at investigating civil and criminal matters in the financial, insurance, entertainment, and real estate industries and on behalf of law firms. Additionally, Mr. Belmont has provided security-consulting services to corporate clients for personal and public events and has completed numerous vulnerability surveys, threat assessments, and crisis management engagements.

As a trial attorney, Mr. Belmont represented large corporations in litigation. Mr. Belmont specialized in fraud, premises liability, labor law and products liability cases. He successfully tried and won verdicts on behalf of Greyhound and Allied Security and prevailed in numerous matters involving fraud against insurance companies.

In addition to his experience as an attorney, Mr. Belmont served as a police officer in Mesa, Arizona. He received his B.A. in Criminal Justice from The George Washington University and his J.D. from Benjamin N. Cardozo School of Law.

PRESTON BYRNE, ESQ.

Biography

Preston Byrne is a banking and securities lawyer in the City of London, specializing in securitization and derivatives. He advises the ASI on legal aspects of its policy proposals and writes on a range of subjects including housing and planning law, the security state, freedom of expression and cryptocurrency.

Preston often contributes to or is quoted by mainstream news media. In 2013, he was the lead author of *Burning Down the House*, the ASI's paper opposing the Conservatives' Help to Buy mortgage subsidy programme, which was covered by hundreds of national and international media outlets including Forbes, the Financial Times, City A.M., Reuters, the Telegraph, the New Statesman, Sky News, Deutsche Welle, and the BBC. More recently, he provided a contributing interview in the book *Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management.* He holds a M.A. in International Relations from the University of St. Andrews and a LL.B. from the College of Law.

JENNIFER CONNORS, ESQ.

Biography

Jennifer Connors is a New York financial services attorney who represents broker-dealers, alternative trading systems (ATSs), financial technology (FinTech) companies and other market participants on securities law and market regulation matters. Ms. Connors' practice has a particular emphasis on broker-dealer regulation and compliance issues, trading rules, issues regarding ATSs, electronic trading, cybersecurity, sales practices and anti-money laundering (AML) rules. She also advises FinTech companies and fund management clients with respect to broker-dealer regulation issues, as well as securities offerings and private placements.

In addition, Ms. Connors regularly counsels clients on U.S. Securities and Exchange Commission (SEC) and Financial Industry Regulatory Authority (FINRA) inquiries and examinations, and continuing membership applications (CMAs). She also handles aspects of regulatory examinations and authorizations administered by select non-U.S. regulators, including the United Kingdom Financial Conduct Authority and the Securities and Futures Commission of Hong Kong.

Ms. Connors has more than 20 years of experience in legal and compliance roles at both global financial services firms and innovative FinTech companies. In these roles, she developed comprehensive written supervisory procedures (WSPs) and training programs for brokerage personnel, and served as a key liaison with financial industry regulators. In addition, Ms. Connors has drafted and negotiated vendor agreements, technology license agreements and electronic-access and trading agreements within the context of a FinTech startup.

Prior to joining Holland & Knight, Ms. Connors was a New York financial services attorney for an international law firm.

MATTHEW D'AMORE

Biography

Matthew D'Amore is a Professor of Practice at Cornell Tech and in the Law School at Cornell University, and currently serves as an Associate Dean at Cornell Tech. D'Amore comes to Cornell after a 20-year career at the international law firm of Morrison & Foerster, where he represented high technology and life-sciences clients in the resolution of complex intellectual property disputes and in licensing matters. In addition to his work for technology clients, D'Amore has been recognized for his *pro bono* work in impact cases for children denied special education services and for citizens deprived of the right to vote, and has served as an adjunct professor at Cornell Law School. Now at Cornell Tech, D'Amore brings his legal industry experience to the Cornell Tech community, teaching Technology Transactions and Trade Secret Law and Practice. D'Amore received his B.S., with distinction, from the Cornell University College of Agriculture and Life Sciences, in biology and society, and his J.D. from Yale Law School.

NED GANNON

Biography

As a co-founder and CEO of eBrevia, Ned Gannon drives the strategic direction of the company and is responsible for overall management. eBrevia uses machine learning technology to improve the efficiency and accuracy of contract review. Ned brings a broad range of legal and business experience to the company. While practicing corporate law with Paul, Hastings, Janofsky and Walker LLP and LeBoeuf, Lamb, Greene & MacRae LLP (n/k/a Dewey & LeBoeuf LLP), Ned represented private equity funds, strategic investors, venture capital funds and startup companies in mergers, acquisitions, financings and general commercial matters. Prior to practicing corporate law, Ned worked in a sales and business development role at Survey Sampling, Inc., a privately-held data collection company. Ned was selected by Capterra as one of five Legal Tech entrepreneurs to watch and speaks frequently on machine learning technology's impact on the legal industry. Ned holds a Juris Doctor from Harvard Law School, a Master in Public Administration from Harvard's Kennedy School of Government and a Bachelor of Science from Boston College.

DIANE HOLT, ESQ.

Biography

Diane Holt is the managing editor of Bloomberg BNA's DealMaker, the Bloomberg Law product for transactional lawyers. Previously, she worked for many years as a corporate lawyer in Europe. She served as international transactional counsel for Enel, SpA, the Italian electric monopoly, in Rome, Italy. She has also worked with a number of Central European regional operations in transition, and she managed Central European Advisory Group, the regional legal and business consultancy. Ms. Hold is a member of the ABA, the American Society for International Law and the Women's Bar Association of D.C. Her recent volunteer work includes serving as a mediator in the D.C. Superior Court, representing at-risk children in family law disputes with the D.C. Volunteer Lawyers Project and mentoring law students. A graduate of Wesleyan University, she earned her JD. at the University of Michigan.

JAKKI KERUBO

Biography

Jakki Kerubo holds an MFA in Creative Writing from New York University (NYU), where she served as an assistant interview editor on the *Washington Square Review*. She has taught non-fiction writing at NYU and the Center for Faith and Work, where she was a 2016 Artist-in-Residence. In the past, Jakki worked as a journalist in the Philippines and in Kenya. There, she covered health, finance and technology and interviewed diverse leaders, including Graca Machel Mandela and Pulitzer Prize-winning author Edwidge Dantica. Her writing has been published in the *Wall Street Journal*, *Quartz*, *Huffington Post*, and the *Golden Handcuffs Review*. A blockchain enthusiast, Jakki hosts workshops to educate others on the basics of this wildly speculative technology. She's the founder of Novum Communications Consulting, and currently works as a communications strategist for both a New York City agency and a blockchain startup. She has a forthcoming debut novel and a non-fiction work in progress.

PERY D. KRINSKY, ESQ.

Biography

PERY D. KRINSKY is the principal of KRINSKY, PLLC, where he focuses his practice on ethics-based defense litigation. Before forming his own law firm, Mr. Krinsky was associated with the law firm of LaRossa & Ross, and then the Law Offices Of Michael S. Ross.

MR. KRINSKY'S ethics-based defense litigation practice focuses on:

- Federal & State Attorney/Judicial Ethics Matters, including: representing attorneys and law firms under investigation by disciplinary authorities and other government agencies; providing guidance to lawyers concerning the day-to-day practice of law; representing disbarred and suspended attorneys seeking reinstatement; advising and representing members of the New York State Judiciary in matters before the New York State Commission on Judicial Conduct; and assisting law school graduates in the admissions process.
- Federal & State Criminal Defense Matters, including: defending clients against law-enforcement actions such as claims of securities fraud, antitrust, investment advisory fraud, health care fraud, tax issues, money laundering, RICO, and narcotics trafficking, among others; helping conduct internal investigations; addressing compliance issues; and responding to regulatory inquiries.
- Art Law Ethics & Litigation Matters, including: allegations of business fraud; art-related disputes; fraudulent transactions; provenance and authenticity; fraudulent inducement to sell; and sales tax evasion.

MR. KRINSKY is a frequent lecturer on topics involving ethics in litigation, personal and professional responsibility and academic integrity, including at: the N.Y. State Judicial Institute; the Appellate Divisions, First and Second Judicial Departments; the N.Y. State Bar Association; the N.Y. City Bar; the N.Y. County Lawyers' Association; the N.Y. State Academy of Trial Lawyers; the N.Y. State Trial Lawyers Association; the Practicing Law Institute; the Bay Ridge Lawyers Association; the Queens County Bar Association; Sotheby's Institute of Art; and law schools such as Brooklyn Law School, Columbia Law School and Fordham Law School.

MR. KRINSKY serves as the Chair of the Ethics Committee of the Entertainment, Arts & Sports Law Section of the N.Y. State Bar Association; and the Chair of the Committee on Professional Discipline of the N.Y. County Lawyers' Association. Mr. Krinsky serves on the Board of Advisors of the N.Y. County Lawyers' Association Institute of Legal Ethics; and is also a Member of: the Brooklyn Bar Association; the N.Y. State Bar Association's Committee on Attorney Professionalism; the N.Y. City Bar Association's Professional Responsibility Committee; and the N.Y. County Lawyers' Committee on Professional Ethics.

JOSHUA KRUMHOLZ, ESQ.

Biography

Joshua Krumholz is a trial attorney who focuses primarily on intellectual property litigation, with a particular emphasis on patent litigation. His practice covers a variety of technologies and jurisdictions. Mr. Krumholz has successfully taken cases to jury verdict in the Eastern District of Texas, Illinois, Massachusetts, New York and New Jersey, among other jurisdictions. Technologies that Mr. Krumholz handles include telecommunications, software, hardware, electronics and consumer goods. His complex commercial experience includes partnership tax disputes, escheatment, healthcare disputes and antitrust matters. Mr. Krumholz represents leading companies across a range of industries, including Ericsson, Verizon, T-Mobile, Avaya, Acushnet (Titleist) and Hasbro, among others.

Intellectual Asset Management (IAM) Patent 1000 has recommended Mr. Krumholz since 2014. The 2017 publication describes him as "…the model lawyer. He can think on his feet before a judge or in a deposition, and his attention to detail is incredible. He has a knack for explaining complex technical issues in plain English, which is the sign of a first-rate trial lawyer. Plus he's always really responsive and focused on cost efficiency – excellently managing the other members in his litigation team." Mr. Krumholz was awarded the Client Choice Award for Massachusetts in 2015, and regularly is honored by Chambers USA and Best Lawyers of America, among other organizations.

GREGORY PICCOLO

Biography

Gregory Piccolo is a Technology Consultant specialized in the architecture, implementation and deployment of blockchain and cryptocurrency backed applications.

An early adopter of Bitcoin and Ethereum technology, Gregory has been the lead engineer on several high-profile corporate blockchain projects across multiple sectors. Most recently and representing IBM, Gregory led development on the highly publicized Trustchain Jewelry initiative.

Gregory is a life-long resident of New York City and is currently based in downtown Manhattan.

T. ALEXANDER PUUTIO, ESQ.

Biography

T. Alexander Puutio is an IP and competition attorney currently working for the United Nations Headquarters in New York. Alexander's current Ph.D. and degree studies at University of Turku and London School of Economics and Political Science involve assessing the complex interplay between competition law and intellectual property, and he devotes much of his research to analysing international aspects of policies that drive financial markets and economic activity at large. He is currently finishing his LLM at Brooklyn Law School. All views expressed are his own and do not in any way reflect those of his institutional affiliations.

RORY RADDING, ESQ.

Biography

Rory Radding is a member of the Locke Lord's Intellectual Property group. He is Co-Chair of the Firm’s ITC Practice Group and former Co-Chair of the Trademark, Copyright and Advertising Practice Group. He has litigated diverse patent, trademark, copyright, and trade secret cases, acting for both plaintiffs and defendants, involving LED lighting and lighting systems, plastic manufacture, electrochemical devices, ring laser gyroscopes, avionics, medical devices, communications, pharmaceuticals, computer controllers, food equipment, data compression, impact sensors, bicycles, candy, wine, jewelry, personal consumer products, television commercials, and vehicle tires; to name a few.

Prior to joining the Firm, Rory was head of the Intellectual Property practice in New York for Morrison & Foerster. Prior to that, he was a senior partner at Pennie & Edmonds, where he practiced for 30 years. Before the start of his legal career, Rory was a pharmaceutical chemist at Wellcome Research Laboratory, and an environmental chemist at Union Carbide Corporation.