NYSBA

Cutting Edge Technologies and Your Practice

What Lawyers Need to Know Today to Prepare for the Digital Future

Thursday, December 6, 2018
NYC

9:00 a.m. – 4:35 p.m.

7.5 MCLE Credits | 6.5 Areas of Professional Practice, 1.0 Ethics

Sponsored by the Committee on Continuing Legal Education, the Committee on Technology and the Legal Profession, and the Law Practice Management Committee of the New York State Bar Association

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. Further, the statements made by the faculty during this program do not constitute legal advice.

NYSBA

Program Description

This program will examine data protection for your firm and clients, blockchain and cybercurrency, crowdfunding and initial coin offerings, as well as navigating the "dark web".

Program Agenda

8:30 a.m. **Registration**

9:00 a.m. – 9:10 a.m. **Welcome and Introductions**

9:10 a.m. – 10:00 a.m. **Cybersecurity and Data Protection for your Firm and Clients**

This panel will discuss the current landscape of cyber security threats to law firms and will address measures that law firms can implement in order to minimize the risk of cyber-attacks and damage, including educating your attorneys and staff, which generally can eliminate over 90% of cyber security attacks, as well as technical issues and the need to have appropriate cyber security insurance.

- Cybersecurity Threats to Law Firms
- How to Defend your Firm and Clients Against the “Dark Arts”
- Educating your Attorneys and Staff
- Should you get Cyberinsurance?

Mark A. Berman, Esq., Ganfer Shore Leeds & Zauderer LLP
Marian C. Rice, Esq., L’Abbate, Balkan, Colavita & Contini LLP
John Bandler, Esq., Bandler Law Firm PLLC
(1.0 Professional Practice)

10:00 a.m. - 10:50 a.m. **Blockchain and Cybercurrency**

- The Benefits of Blockchain, Including Immutability and Reducing Fraud in Transactions
- Different Types of Tokens: When a Token is not Currency
- Use Cases In Auditing and Financial Services
- Case Study: Blockchain and Paying for Cannabis, using Cryptocurrency as a way of Working around Banking Limits

Mayling C. Blanco, Esq., Blank Rome LLP
Scott E. Wortman, Esq., Blank Rome LLP
Kevin Hart, Founder and President, Green Check Verified
Erin Plante, Inventus
(1.0 Professional Practice)

10:50 a.m. - 11:00 a.m. **Break**

11:00 a.m. - 11:50 a.m. **Crowdfunding and Initial Coin Offerings**

- Equity Crowdfunding Under Title III of the JOBS Act and Regulation Crowdfunding Two Years Later
- Can you still Crowdfund the “Old Fashioned” Way without Title III?
- Resources for Assisting Clients in Crowdfunded Offerings
- Initial Coin Offerings: Where they are Legal, How they are Regulated, and how to Structure an Offering to Minimize Regulatory Risk

Cliff Ennico, Esq., Law Offices of Clifford R. Ennico
(1.0 Professional Practice)

11:50 a.m. - 12:35 p.m. **Lunch (on your own)**

12:35 p.m. - 1:25 p.m.

Artificial Intelligence and the Law

- What is “Artificial Intelligence” (“AI”) and How Does It Work?
- What Legal AI Applications are Available Today?
- What are Some of the Benefits and Challenges of AI?
- How Can a Lawyer Vet AI Tools for His or Her Practice?

Ignatius A. Grande, Esq., Berkeley Research Group, LLC
Scott B. Reents, Esq., Cravath, Swaine & Moore LLP
(1.0 Professional Practice)

1:25 p.m. - 2:15 p.m.

Technology Assisted Review for eDiscovery

- What is “Technology-Assisted Review” (“TAR”) and what are the Different Types of TAR Available Today?
- How Do We Know that TAR is better than Search Terms or Manual Review?
- What Have the Courts Said About TAR?
- What are some of the Benefits and Challenges of TAR?

Ignatius A. Grande, Esq., Berkeley Research Group, LLC
Jason Lichter, Esq., Pepper Hamilton LLP
(1.0 Professional Practice)

2:15 p.m. – 2:30 p.m.

Break

2:30 p.m. – 3:20 p.m.

Navigating the “Dark Web”

- What does the “Dark Web” Already Know About you, your Firm and Clients?
- How to Keep your Data Off the “Dark Web”
- What to do if the “Dark Web” gets Hold of Sensitive Data

Mary J. Hildebrand, Esq., Founder & Chair, Privacy and Cybersecurity Practice
(1.0 Professional Practice)

3:20 p.m. – 4:10 p.m.

Ethical Implications of Cutting-Edge Technologies

- What Does “Competence” Mean When it comes to New Technologies?
- What Does “Supervision” Require in the Context of New Technologies?
- What are Reasonable Attorneys’ Fees When it Comes to the Use of New Technologies?

Roundtable Discussion:
Mark A. Berman, Esq., Ganfer Shore Leeds & Zauderer LLP
Cliff Ennico, Esq., Law Offices of Clifford R. Ennico
(1.0 Ethics)

4:10 p.m. – 4:35 p.m.

Panel Discussion: New Technologies and the Lawyer of the Future: Adapting Your Practice to a Digital World

- Are New Technologies Only for Large Firms or Can they be Useful to Small Firms As Well?
- How Does a Lawyer Vet New Technologies?
- What Will the Law Firm of the Future Look Like?

Roundtable Discussion:
Mark A. Berman, Esq., Ganfer Shore Leeds & Zauderer LLP
Cliff Ennico, Esq., Law Offices of Clifford R. Ennico
(0.5 Professional Practice)

4:35 p.m.

Adjournment

Accessing the Online Course Materials

Below is the link to the online course materials. These program materials are up-to-date and include supplemental materials that were not included in your course book.

www.nysba.org/CuttingEdgeTechMaterials/

All program materials are being distributed online, allowing you more flexibility in storing this information and allowing you to copy and paste relevant portions of the materials for specific use in your practice. WiFi access is available at this location however, we cannot guarantee connection speeds. This CLE Coursebook contains materials submitted prior to the program. Supplemental materials will be added to the online course materials link.

Follow Law Practice Management on Twitter for Quick and Relevant Program Information!

New York Rules of Professional Conduct

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).

http://nycourts.gov/rules/jointappellate/NY-Rules-Prof-Conduct-1200.pdf

Free, Confidential Help for the Problems Lawyers Face

NYSBA Lawyer Assistance Program

1.800.255.0569 | nysba.org/LAP

All LAP services are confidential and protected under Section 499 of the Judiciary Law as amended by Chapter 327 of the Laws of 1993.

NYSBA
CLE
2018
Live & Webcast Programs

NYSBA
Law Practice Management

Table of Contents

Cutting Edge Technologies and Your Practice: What Lawyers Need to Know Today to Prepare for the Digital Future

NYSBA

Table of Contents

Cutting Edge Technologies and Your Practice: What Lawyers Need to Know Today to Prepare for the Digital Future

NYSBA

Table of Contents

Cutting Edge Technologies and Your Practice:
What Lawyers Need to Know Today to Prepare for the Digital Future

Topic I

Cybersecurity and Data Protection for Your Firm and Clients

ABA JOURNAL Since 1915

Home / In-Depth Reporting / Prepare for and plan against a cyberattack

DIGTIAL DANGERS

Prepare for and plan against a cyberattack

BY JOHN BANDLER

JULY 2018 (/MAGAZINE/ISSUE/2018/07/)

Like Tweet LinkedIn submit

Imagine this (not-so-outlandish) scenario: Your law practice has suffered a data breach. Your email accounts, computers or networks have been compromised and your confidential data is no longer confidential. It doesn't matter how it happened—whether it was a cyberattack, a phishing scam or simply human error. If you are the victim, then you have to respond and protect yourself, your firm and your clients from further harm. If your client was victimized, you might get a frantic call seeking advice.

The best and most effective way to avoid a worst-case scenario is to have a structure already in place to deal with and respond to cyberincidents. Failure to prepare is preparation for failure, and lawyers must invest time toward incident response planning before a breach occurs. Planning for a data breach may seem less fun than preparing for a serious traffic collision, but it comes with benefits that include knowledge, prevention and better response. Contemplating the consequences of a serious cybercrime allows us to properly allocate time and money toward avoiding it.

Good incident response planning and good cybersecurity go together and are continual processes. Planning starts before the breach—just like driver's education starts before the imminent traffic accident. When it is time to take emergency evasive action, you already should know how to use the steering wheel and brake. After the collision, you should know what to do, including whether you are allowed to leave the scene or must notify the police.

The threats and risks are clear: Our profession makes us targets, and we have special duties of confidentiality and competence. Attorneys are subject to frequent cybercrime attacks, email accounts are breached, and we are solicited to move

Illustration by Lightspring/Shutterstock.com.

money for cybercriminals. Law firms have been breached, their secrets exposed to the world or used for insider trading—the Panama Papers, the Paradise Papers and other events speak to that. Knowledgeable lawyers can protect themselves and their clients.

BREACH RESPONSE OVERVIEW

For background, consider the computer security incident-handling steps from the National Institute of Standards and Technology, outlining four cyclical phases of incident response beginning before the commission of a cybercrime: preparation; detection and analysis; containment, eradication and recovery; and post-incident activity.

The NIST cybersecurity framework also envisions a continual process through identifying operations, assets and data; protecting on a risk-prioritized basis; detecting cybersecurity events; responding to them; and recovering from them.

These are helpful frameworks for information security professionals, and this article adapts them for your incident response planning.

PREPARE FOR THE CYBERCRIME

Before disaster strikes, develop foundational knowledge and improve your cybersecurity posture in your personal and work lives. To get started, read my article in the ABA's September/October 2017*GPSolo* magazine, "Cybercrime and Fraud Protection for Your Home, Office, and Clients."

DIGITAL DANGERS

Cybersecurity and the law

A joint production of the ABA Journal and the ABA Cybersecurity Legal Task Force

Develop an incident response plan. Perform risk analysis, evaluate threats, consider probabilities and potential harms, and think about how you would respond. Ask three questions to address the critical information security concepts of confidentiality, integrity and availability.

1. What confidential information do I store, where is it, and what would happen if it were stolen? Think data breach.

2. What harm could a hacker do by tampering with my systems, including by hacking my email account and sending emails as if he were me?

3. What information and systems are essential? What if I could no longer access them? Consider a ransomware attack.

Think about your incident response procedure and whether it is periodically reviewed, practiced and updated. If nothing is written down, consider getting started with a list, plan or call tree.

Which people are required to respond to an incident, inside and outside your organization? Identify them and their roles and responsibilities ahead of time, and ensure the team can contact one another in a crisis. They should include: designated incident handler; legal counsel; public relations; information technology; digital forensics investigation and recovery; insurance; and law enforcement and other government agencies.

DETECTING A BREACH OR FRAUD

When anomalies occur, we have to know about them and determine whether they are merely an event or a serious incident. We are all important sensors, whether or not we work in a large organization that has tools and personnel dedicated to detecting and preventing a data breach—and especially in smaller organizations.

Attorneys and our clients may need to rely upon our wits, knowledge, communication skills and the ability to review and configure our applications. Again, this starts before the breach. Checking the settings for our applications is as important as turning the lock on our door or setting the burglar alarm. If we fail to do this properly, our tools are ineffective.

We should periodically review the security and privacy settings for our email and cloud accounts and configure them to alert us when there is suspicious activity. We have to discern genuine alerts from fraudulent phishing attempts and be aware of suspicious behavior from our devices and the people we communicate with. Yes, people, too. After all, people can be easily impersonated, and their email accounts can be easily hacked.

Pick up the phone and have a verbal conversation when in doubt. This improves security, combats social engineering, and builds personal relationships. We should warn our clients of fraud risks, including business email compromise and bank wiring scams.

Read more ... (http://www.abajournal.com/magazine/article/prepare_plan_against_cyberattack/P1)

1 **2** Next Page

ABA JOURNAL Since 1915

Home / In-Depth Reporting / Prepare for and plan against a cyberattack

DIGTIAL DANGERS

Prepare for and plan against a cyberattack

Like Tweet LinkedIn submit

IMMEDIATE STEPS

Consider containment, mitigation, eradication and investigation. Stop the crime from getting worse, minimize further damage, and preserve evidence. Get the attackers and infections out of your system so you can resume normal operations.

There will be tension related to the competing needs to (1) contain a breach, (2) proceed rapidly toward recovery and resumption of normal business operations, (3) minimize expenditure of time and funds, and (4) investigate and collect evidence. Faced with the same set of circumstances, each individual or organization will have a unique response.

Photograph of John Bandler by Gail Bandler.

Professionals have the best tools and skills to preserve evidence, but this costs money and it takes time until they are on scene. Computing devices have permanent storage that can be forensically copied (imaged) for future analysis and evidentiary use. Applications and viruses running in volatile memory can be documented so long as the computer has not been turned off.

Beyond forensic techniques, we can preserve evidence by taking pictures, making notes and obtaining screen grabs, which is better than doing nothing at all. We should save all relevant emails, especially those to or from the criminal.

DIGITAL DANGERS

Cybersecurity and the law

A joint production of the ABA Journal and the ABA Cybersecurity Legal Task Force

Containment may require disconnecting infected devices from the network and internet and possibly turning them off (realizing some evidence may be lost). Ultimately, you will decide whether the device should be forensically imaged for evidence, can be properly cleaned or should be destroyed.

Containment and eradication include regaining exclusive control of cloud accounts and making sure that intruders don’t have access. Review the settings in cloud accounts, check recent logins and security settings, change passwords, enable two-factor authentication, and contact the provider.

Notification of law enforcement and potential victims can be an important mitigation step, even if it is not yet legally required. If funds have been stolen, notify the bank and law enforcement immediately, including the FBI. There is a chance the funds can be recovered if you work fast. If an email account was hacked, criminals might attempt social engineering frauds based on information within the account. So warn potential victims to alert them to this risk.

Recovery means getting the systems and business back to normal operation. This might require reconnecting to the network, restoring backups, setting up new computers, and properly testing them. An impartial and objective investigation can learn helpful facts to further the criminal investigation, determine root causes and security weaknesses, and help apportion fault or liability.

Further, when funds are stolen or businesses are damaged, stakeholders will want to know how and why it occurred, and business and legal decisions should be grounded in accurate information. Attorney-supervised investigations may have the additional benefit of being legally privileged.

NOTIFICATIONS AND LESSONS LEARNED

Consider legal duties of notification to the government and victims. Most states have data-breach reporting laws, requiring notification to law enforcement, the state attorney general, and individuals whose personal information was accessed or stolen (potentially customers, clients and employees).

If you already notified some of these parties as a mitigation step, now is the time to ensure legal obligations are complied with. Look to the laws of your home state and to other states where you operate or have clients.

If a law firm is breached, be mindful of fiduciary duties owed to current and former clients. There can be a conflict between the attorney's self-interest (in preserving the legal practice and avoiding a claim) and the client's interests. This would make it difficultfor the attorney to provide unconflicted advice to the client about how to proceed.

After the crisis has passed, with the benefit of hindsight and new experience, take time to improve defenses and incident response procedures. Many skip this step, exhausted from the incident or wrongly thinking lightning never strikes twice in the same place. Cybercrime is attracted to weak cybersecurity and fraud defenses, like lightning, are attracted to tall, conductive objects.

Preparation and planning will help you respond effectively to a data breach or a cybercrime and perhaps prevent one from occurring. Your incident response plan should be part of a broader cybersecurity program, which starts with improving your knowledge and awareness.

Previous Page | 1 | 2

John Bandler is the founder of the Bandler Law Firm in New York City, which helps firms, businesses and individuals with cybersecurity, cybercrime investigations, litigation support and other areas. He is the author of the ABA-published book Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security (https://shop.americanbar.org/eBus/Store/ProductDetails.aspx?productId=283993925), *which includes sections on incident response planning and procedures.*

This article was published in the July 2018 ABA Journal *magazine with the title: "Preparing Today for Tomorrow's Attack: A cybersecurity expert details how to prepare for and plan against a cyberattack."*

NEW YORK STATE BAR ASSOCIATION

Journal

NYSBA

JULY/AUGUST 2018

VOL. 90 | NO. 6

A NEW YORK STATE OF MARIJUANA

CONNECT WITH NYSBA
VISIT NYSBA.ORG/BLOG

A Current Look at Cannabis Law

MEDICAL MARIJUANA IN THE WORKPLACE

COUNSELING MARIJUANA CLIENTS ON IP PROTECTION AND ENFORCEMENT

MURPHY V. NCAA & MARIJUANA

ROCKEFELLER DRUG LAWS

LAW PRACTICE MANAGEMENT:
CYBER SECURITY RISKS ATTORNEYS FACE DAILY

A Day in the Life of an Attorney: The Cybersecurity, Technology, and Crime Risks We Face

By John Bandler

Attorneys face cybercrime threats every day that jeopardize our practice, clients, and family. This is true for solo practitioners and members of large firms, representing individuals or multi-national conglomerates, and in all practice areas. Knowledge, awareness, and effort are required to protect from cybercrime and fraud threats.

Let's review a day in the life of Lex, our fictional lawyer, to illustrate the threats to our professional and personal lives, and see how crime, cybersecurity, information security, technology, and safety are related and enmeshed in our lives.

THE DAY BEGINS

It is midnight so the calendar day has officially begun, but Lex and his family are asleep. His home is quiet, as is the neighborhood. Lex is an attorney in a small firm, handling many legal issues for his clients.

Elsewhere, the worldwide cybercrime economy is hard at work across every time zone. Some cybercriminals are awake and at work on their schemes. Others have set in motion computer programs to perform malicious work without ever needing rest – so called "bots." These cybercriminals collectively control an army of computers throughout the world, many of them infected with malware and transformed into malicious tools without their owners' knowledge.

One program is trying to gain access and compromise the administrator portals of millions of websites, one of which is LexLaw.com. First it tries to log in as user "admin," with a password of "admin," but access is denied because this is not the website's username and password. It tries a different guess, is denied, and the process continues.

A different program attempts to log into email accounts, including Lex's work and personal email accounts. Lex's passwords are long and complex, and are unlikely to be guessed by this program. He also uses two-factor authentication, which means that guessing the password is not enough – the hacker would need possession of Lex's smartphone to get the one-time code from his email provider.

A third bot has been scanning the internet looking for connected devices. It finds Lex's home internet connection, starts to communicate with his router, and tries to gain access. It goes through a list of default usernames and passwords (including username "admin" and password "admin") but is unsuccessful and keeps trying. It runs through a sequence of hacking attacks but that doesn't work either. Recently, Lex updated his router's firmware to patch it against these vulnerabilities, and he also rebooted it according to the FBI's May 2018 advisory, a step which could help ensure it is not infected by malware.

Lex's children are sleeping, their smartphones and laptops are off and charging in the living room. The children are frequently tempted to check their devices, but know this is not allowed at night. However, some of their classmates are still awake and communicating with each other by social media, text, and email. Some messages are funny and harmless, but some are cruel or inappropriate, and all of them are sacrificing rest and relaxation.

Nearby, someone is trying to gain access to Lex's Wi-Fi network through password guessing, and is also attempting to access the network administrator portal. Whether this person merely wants to borrow Lex's internet connection or do something nefarious is unknown, but fortunately the Wi-Fi password is long and complex, and the router is patched.

LEX WAKES UP

At 6 a.m. Lex's alarm rings and he is up before the family. He logs into his computer and then checks LinkedIn, which prompts him to boost his contacts. That sounds like a great idea, so he clicks the button to accept the suggestion, is prompted for a password so he enters his LinkedIn password, but gets an error message. By now he realizes that LinkedIn wants the password to his email account, which fortunately is different from his LinkedIn password. It would have been unfortunate to give LinkedIn access to his email account and its contents, and for automatic invitations to have been sent all over.

Lex reviews an email he drafted last night, summarizing legal options for a client. After some final touches it is ready to send so he types the first few letters of the client's name into the "To" field, then hits enter for the autocomplete function to fill in the address. He is about to hit "Send" when he takes a last look and realizes he is about to send it to the wrong person! That would have been disastrous, so he corrects the email address, takes another look to confirm, and then sends it on its way. He wonders if this day will be a continual test of his information security knowledge and awareness.

Lex gets ready, says goodbye to his spouse and children, starts the drive to the office and then receives a call from Janet, his client in a pending real estate transaction. She is buying a home and wants to know if there are any updates on the closing. Lex tells her the recently scheduled date, and they discuss the details.

> **Lex**: Janet, remember what I told you when you first retained me. Any payment instructions will be confirmed with a phone conversation between us. Any changes to those payment instructions will also be confirmed by phone.

Janet laughs and says she remembers his earlier warning about this fraud risk, sometimes known as "business email compromise" or "CEO fraud." She promises not to rely on an email, since emails can be hacked or spoofed.

Lex had conducted this call while keeping his hands free and ensuring sufficient attention is devoted to the dangerous task of driving the car. After they hang up, Lex feels his smartphone vibrating and is tempted to check it, but resists. The constant demands of technology upon our attention and concentration are a challenge, but he soon reaches his destination and checks his text and email messages.

He is representing a client in a contract dispute where the settlement offer was accepted and the attorney for the opposing party has now emailed payment instructions. He asks that Lex's client wire the funds as soon as possible to the account provided, and indicates he is unavailable to talk by phone. Lex is about to forward the instructions to his client, but decides to wait and verify the instructions. Soon, he is in his office and calls opposing counsel.

> **Lex**: Hi Michael, Lex here. I got your email, I just wanted to confirm a few things.
>
> **Michael**: Hi Lex, what email?
>
> **Lex**: The email you sent me with the bank wiring instructions.
>
> **Michael**: Impossible, I didn't send that. I am still waiting to hear back from my client.
>
> **Lex**: You didn't send me an email 15 minutes ago?
>
> **Michael**: No, I didn't send anything.

Clearly, something is not right. Someone has impersonated Michael and knew a lot about this pending transaction. Fortunately, Lex knows what to do, and the two discuss their next steps. (You can learn this too, in an upcoming NYSBA *Journal* article.)

Lex is meeting a colleague at a local coffee shop, gets there first, grabs a table by the window and checks his phone. He

John Bandler **helps firms, businesses, and individuals with cybersecurity, crime prevention, and investigations. He is former prosecutor and police officer, and the author of the comprehensive book, "Cybersecurity for the Home and Office." You can find him online at: https://cybersecurityhomeandoffice.com or https://bandlerlaw.com. LinkedIn: www.linkedin.com/in/johnbandler.**

is frustrated by the slowness of his cellular service and the shop offers free Wi-Fi, which Lex considers using. But then his imagination starts working; he wonders if another customer in the coffee shop might be a malicious hacker, and whether the coffee shop maintains their Wi-Fi network securely. Have they heeded the FBI advisory or patched their router? Lex knows that connecting to public Wi-Fi networks has risks, and decides that today it is not worth it.

Just then, he receives a text from Bill, who is on the way and asks that Lex get his coffee. Lex gets up, makes the purchase, and as he is returning to the table he panics. He realizes that he had left his cell phone on the table and his laptop in his bag under the table. As he walks back quickly he sees that his phone is no longer on the table, and his bag with the laptop is missing. His mind is racing because he is not sure if he locked the phone before he got up – maybe right now the thief is sifting through all of his emails and contacts? Then he looks to the side and sees Bill, staring at him with a mischievous smile while holding Lex's phone in one hand, and briefcase in the other.

> **Bill**: Hi there Lex, you look nervous! Don't you remember learning that the first principle of information security is maintaining physical security of your computers?

Bill is right; that was one of the many gems of knowledge contained in the book they both read, *Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security*." Bill absorbed all of the practical information in the book, and now re-reads it periodically to savor the mellifluous prose. (Remember, this article is a work of fiction, with occasional attempts at humor and shameless puffery.)

> **Lex**: Bill, you are right, but this has been a tough day for me. An hour ago, a fraudster tried to redirect a bank wire, and I almost forwarded those instructions to my client. Last night I had a dream about botnets and automated password attacks, and now you give me heart palpitations with this prank, after I bought your coffee.

Bill apologizes but Lex concedes it was a good lesson, and they both discuss the potential implications if Lex's smartphone or laptop were stolen. It affects all three of the main information security principles– confidentiality, integrity, and availability. What data could the thief have accessed? What if the thief could send emails from Lex's system, and alter data? How would Lex's access to his data be affected? They agree on the importance of keeping possession of one's devices, and locking them after use.

After they say goodbye, Lex gets a call from Sandra, who is in charge of training at his firm.

> **Sandra**: Hi Lex, how is your day going so far? Quick question. Is there a connection between attorney professional responsibility, cybersecurity, and technology?

> **Lex**: There certainly is! Think about the attorney duties of competence and confidentiality. See the NYS Rules of Professional Conduct and the ABA Model Rules, especially...

> **Sandra**: Do you know of any training that covers those?

> **Lex**: Yes, I saw a CLE on cybersecurity for lawyers. Protecting yourself, your clients, and your family from cybercrime, privacy, and fraud threats. It was fantastic. I got two ethics credits and knowledge which I am putting to use today.

> **Sandra**: Thanks. Send me the information and I'll check it out. Maybe we can do something for the firm. See you later.

Lex returns to the office until noon, then goes to his parents' house for their weekly lunch. As soon as he gets in the door he receives a text from a colleague about to send a letter but requesting a final review. Lex considers his options: His smartphone screen is tiny but his parents have a computer which is well maintained – thanks in part to Lex – so he decides it is safe enough to use for this purpose (unlike a computer in a library or hotel).

Lex launches the web browser in a "private" or "incognito" window so that the computer will not store too much information about his activity. He navigates to his law firm's web portal and enters his username and password, which is not enough to gain access because his firm has implemented multi-factor authentication. Lex is prompted for his one-time code, which he retrieves from his smartphone and types in. He has now proven to the system that he both *knows* his password and *possesses* his smartphone, providing two types of authentication, and the system grants him access. This greatly increases security over passwords alone, which can be guessed or stolen.

Lex accesses the document and reads it, then lets his colleague know that it is good. He "logs out" of his cloud account, then takes a quick look at his parents' computer to make sure it is running properly and safely. He runs a malware scan using reputable free software, and checks that the web browser is updated and not running any unnecessary plug-ins or extensions.

Lex's parents are not getting younger, and they face different cybersecurity and technology challenges compared to his children. It takes effort to ensure that his parents are able to use technology easily, safely, and while staying connected to friends, family, and the world. Pop-up messages, phishing emails, malware, scareware, and technical support scams make computing difficult for everyone, but are especially challenging for seniors. After lunch Lex returns to his office and starts going through his messages.

James, a potential client, has left a message to continue their discussion about his financial institution and the New York State Department of Financial Services regulation called “Cybersecurity Requirements for Financial Services Companies.” Lex calls him back and they talk.

James: Lex, thanks for calling, I’ve got you on speakerphone and with me is Anthony, my general counsel. What do I need to do to comply with this regulation?

Lex: We can help with that, but first we should evaluate your current information security program.

James: I’d rather not get sidetracked with that, because I need to comply with this cybersecurity regulation, and yesterday. I say yesterday in a literal sense, because I must sign a document saying that I complied with the regulation for the past year.

Lex: We should talk about that attestation later. But first we should see how your information security program aligns with what the regulation requires. The regulation is really about information security, not just cybersecurity.

Anthony: Lex, let me interject because I don’t agree. The regulation title says cybersecurity, and the text mentions cybersecurity throughout! Let me count it, 1, 2, 3 . . . [counting continues] . . . 73, 74, 75! Seventy-five mentions of “cybersecurity” and hardly a mention of “information security,” except once in passing, and when spelling out “CISO.” If New York State wanted to issue an information security regulation, that’s what they would have called it, so we have to go by their original intent.

James: Exactly. Besides, is “information security” really important? All I hear about in the news is “cybersecurity” and “cyber,” so I think we should focus on that.

Lex explains that the rule addresses all aspects of information security, which encompasses cybersecurity, making the case that it is an information security regulation. Lex speculates why the term “cybersecurity” was used so much in the title and text of the regulation, and suggests that they think holistically under the ambit of “Cybersecurity and Information Security.”

James: That’s very persuasive. Can you give us a quick and free information security lesson?

Lex: Of course. For starters, think “CIA”: confidentiality, integrity, and availability. Keep your data and systems *confidential* and from being hacked or stolen. Ensure they maintain *integrity*, that no one can alter or change information without authorization. And keep them *available*, so that operations can continue and are not subject to outages or disruption. That includes backing up your data.

James: Wow, how did you learn all of that?

Lex: I read a marvelous book about cybersecurity, and it helped me take charge of my information security and help my clients. I can come by, give you a copy, and we can get started on your issues. Are you free at nine tomorrow morning?

James: Sounds good, see you then.

Lex reviews a number of email messages from strangers who are requesting legal representation, each willing to pay lucrative legal fees in exchange for what seems to be some very simple legal work, including:

- Finalizing the settlement documents of a nearly completed deal, receiving the settlement funds and then forwarding them – after keeping a hefty fee – to the client.
- Finalize contract documents for the purchase of equipment, receive the payment, keep a large fee, then forward the remainder to the seller.
- Help several different foreign residents (one of whom is a Nigerian prince) secretly transfer funds out of their respective countries.

Lex spots the indicators of fraudulent schemes – criminals trying to recruit him to receive stolen funds, to act as an unwitting money launderer or “money mule.” He marks these as spam and deletes them. Then Sandra arrives at his office door.

Pop-up messages, phishing emails, malware, scareware, and technical support scams make computing difficult for everyone, but are especially challenging for seniors.

Sandra: Hi Lex, how has your day been? Can you tell me what you think about this cybersecurity training outline for the firm?

- User knowledge and awareness.
- Information security basics: CIA.
- Device security: Don’t lose them, use passwords, and check settings.
- Cloud data security: Use strong passwords and two-factor authentication.
- Back up data and test the backups.
- Business Email Compromise prevention through verbal confirmation of any funds transfer instruction.

Lex: I think you nailed it, perhaps add a section on network security and I will think some more on it. We should buy a dozen copies of this book to give out [*gesturing*], and we should set a date and start fleshing it out.

By now it is time to leave. Lex shuts down his desktop computer, scans his desk and office for any sensitive documents that need to be put away, then makes his way out of the office, saying his goodbyes. The receptionist has left for the day, so the front door has been locked, and Lex makes sure it locks behind him. Information security – and the safety of the firm’s employees – requires good physical security.

It has been a busy day, but Lex feels glad that he has protected himself, his firm, clients, and family from many threats, and looks forward to a relaxing evening at home.

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 483 **October 17, 2018**

Lawyers’ Obligations After an Electronic Data Breach or Cyberattack

Model Rule 1.4 requires lawyers to keep clients “reasonably informed” about the status of a matter and to explain matters “to the extent reasonably necessary to permit a client to make an informed decision regarding the representation.” Model Rules 1.1, 1.6, 5.1 and 5.3, as amended in 2012, address the risks that accompany the benefits of the use of technology by lawyers. When a data breach occurs involving, or having a substantial likelihood of involving, material client information, lawyers have a duty to notify clients of the breach and to take other reasonable steps consistent with their obligations under these Model Rules.

Introduction[1]

Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers.[2] In one highly publicized incident, hackers infiltrated the computer networks at some of the country’s most well-known law firms, likely looking for confidential information to exploit through insider trading schemes.[3] Indeed, the data security threat is so high that law enforcement officials regularly divide business entities into two categories: those that have been hacked and those that will be.[4]

In Formal Opinion 477R, this Committee explained a lawyer’s ethical responsibility to use reasonable efforts when communicating client confidential information using the Internet.[5] This

[1] This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2018. The laws, court rules, regulations, rules of professional conduct and opinions promulgated in individual jurisdictions are controlling.

[2] *See, e.g.*, Dan Steiner, *Hackers Are Aggressively Targeting Law Firms’ Data* (Aug. 3, 2017), https://www.cio.com (explaining that “[f]rom patent disputes to employment contracts, law firms have a lot of exposure to sensitive information. Because of their involvement, confidential information is stored on the enterprise systems that law firms use. . . . This makes them a juicy target for hackers that want to steal consumer information and corporate intelligence.”); *See also Criminal-Seeking-Hacker’ Requests Network Breach for Insider Trading*, Private Industry Notification 160304-01, FBI, CYBER DIVISION (Mar. 4, 2016).

[3] Nicole Hong & Robin Sidel, *Hackers Breach Law Firms, Including Cravath and Weil Gotshal*, WALL ST. J. (Mar. 29, 2016), https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504.

[4] Robert S. Mueller, III, *Combatting Threats in the Cyber World Outsmarting Terrorists, Hackers and Spies*, FBI (Mar. 1, 2012), https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies.

[5] ABA Comm. on Ethics & Prof’l Responsibility, Formal Op. 477R (2017) (“Securing Communication of Protected Client Information”).

opinion picks up where Opinion 477R left off, and discusses an attorney's ethical obligations when a data breach exposes client confidential information. This opinion focuses on an attorney's ethical obligations after a data breach,[6] and it addresses only data breaches that involve information relating to the representation of a client. It does not address other laws that may impose post-breach obligations, such as privacy laws or other statutory schemes that law firm data breaches might also implicate. Each statutory scheme may have different post-breach obligations, including different notice triggers and different response obligations. Both the triggers and obligations in those statutory schemes may overlap with the ethical obligations discussed in this opinion. And, as a matter of best practices, attorneys who have experienced a data breach should review all potentially applicable legal response obligations. However, compliance with statutes such as state breach notification laws, HIPAA, or the Gramm-Leach-Bliley Act does not necessarily achieve compliance with ethics obligations. Nor does compliance with lawyer regulatory rules *per se* represent compliance with breach response laws. As a matter of best practices, lawyers who have suffered a data breach should analyze compliance separately under every applicable law or rule.

Compliance with the obligations imposed by the Model Rules of Professional Conduct, as set forth in this opinion, depends on the nature of the cyber incident, the ability of the attorney to know about the facts and circumstances surrounding the cyber incident, and the attorney's roles, level of authority, and responsibility in the law firm's operations.[7]

[6] The Committee recognizes that lawyers provide legal services to clients under a myriad of organizational structures and circumstances. The Model Rules of Professional Conduct refer to the various structures as a "firm." A "firm" is defined in Rule 1.0(c) as "a lawyer or lawyers in a law partnership, professional corporation, sole proprietorship or other association authorized to practice law; or lawyers employed in a legal services organization or the legal department of a corporation or other organization." How a lawyer complies with the obligations discussed in this opinion will vary depending on the size and structure of the firm in which a lawyer is providing client representation and the lawyer's position in the firm. *See* MODEL RULES OF PROF'L CONDUCT R. 5.1 (2018) (Responsibilities of Partners, Managers, and Supervisory Lawyers); MODEL RULES OF PROF'L CONDUCT R. 5.2 (2018) (Responsibility of a Subordinate Lawyers); and MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018) (Responsibility Regarding Nonlawyer Assistance).

[7] In analyzing how to implement the professional responsibility obligations set forth in this opinion, lawyers may wish to consider obtaining technical advice from cyber experts. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.") *See also, e.g.*, *Cybersecurity Resources*, ABA Task Force on Cybersecurity, https://www.americanbar.org/groups/cybersecurity/resources.html (last visited Oct. 5, 2018).

I. Analysis

A. Duty of Competence

Model Rule 1.1 requires that "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[8] The scope of this requirement was clarified in 2012, when the ABA recognized the increasing impact of technology on the practice of law and the obligation of lawyers to develop an understanding of that technology. Comment [8] to Rule 1.1 was modified in 2012 to read:

> 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. (Emphasis added.)[9]

In recommending the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to 'keep abreast of changes in the law and its practice.' The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document. [10]

[8] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2018).

[9] A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 43 (Art Garwin ed., 2013).

[10] ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase 'including the benefits and risks associated with relevant technology,' would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

In the context of a lawyer's post-breach responsibilities, both Comment [8] to Rule 1.1 and the 20/20 Commission's thinking behind it require lawyers to understand technologies that are being used to deliver legal services to their clients. Once those technologies are understood, a competent lawyer must use and maintain those technologies in a manner that will reasonably safeguard property and information that has been entrusted to the lawyer. A lawyer's competency in this regard may be satisfied either through the lawyer's own study and investigation or by employing or retaining qualified lawyer and nonlawyer assistants.[11]

1. Obligation to Monitor for a Data Breach

Not every cyber episode experienced by a lawyer is a data breach that triggers the obligations described in this opinion. A data breach for the purposes of this opinion means a data event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode.

Many cyber events occur daily in lawyers' offices, but they are not a data breach because they do not result in actual compromise of material client confidential information. Other episodes rise to the level of a data breach, either through exfiltration/theft of client confidential information or through ransomware, where no client information is actually accessed or lost, but where the information is blocked and rendered inaccessible until a ransom is paid. Still other compromises involve an attack on a lawyer's systems, destroying the lawyer's infrastructure on which confidential information resides and incapacitating the attorney's ability to use that infrastructure to perform legal services.

Model Rules 5.1 and 5.3 impose upon lawyers the obligation to ensure that the firm has in effect measures giving reasonable assurance that all lawyers and staff in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2], and Model Rule 5.3 Comment [1] state that lawyers with managerial authority within a firm must make reasonable efforts to establish

[11] MODEL RULES OF PROF'L CONDUCT R. 5.3 (2018); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2018); *See also* JILL D. RHODES & ROBERT S. LITT, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 124 (2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK].

internal policies and procedures designed to provide reasonable assurance that all lawyers and staff in the firm will conform to the Rules of Professional Conduct. Model Rule 5.1 Comment [2] further states that "such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."

Applying this reasoning, and based on lawyers' obligations (i) to use technology competently to safeguard confidential information against unauthorized access or loss, and (ii) to supervise lawyers and staff, the Committee concludes that lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data[12] and the use of data. Without such a requirement, a lawyer's recognition of any data breach could be relegated to happenstance --- and the lawyer might not identify whether a breach has occurred,[13] whether further action is warranted,[14] whether employees are adhering to the law firm's cybersecurity policies and procedures so that the lawyers and the firm are in compliance with their ethical duties,[15] and how and when the lawyer must take further action under other regulatory and legal provisions.[16] Thus, just as lawyers must safeguard and monitor the security of paper files and actual client property, lawyers utilizing technology have the same obligation to safeguard and monitor the security of electronically stored client property and information.[17]

While lawyers must make reasonable efforts to monitor their technology resources to detect a breach, an ethical violation does not necessarily occur if a cyber-intrusion or loss of electronic information is not immediately detected, because cyber criminals might successfully hide their

[12] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008).
[13] Fredric Greene, *Cybersecurity Detective Controls—Monitoring to Identify and Respond to Threats*, ISACA J., Vol. 5, 1025 (2015), *available at* https://www.isaca.org/Journal/archives/2015/Volume-5/Pages/cybersecurity-detective-controls.aspx (noting that "[d]etective controls are a key component of a cybersecurity program in providing visibility into malicious activity, breaches and attacks on an organization's IT environment.").
[14] MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2018); MODEL RULES OF PROF'L CONDUCT R. 1.15 (2018).
[15] *See also* MODEL RULES OF PROF'L CONDUCT R. 5.1 & 5.3 (2018).
[16] The importance of monitoring to successful cybersecurity efforts is so critical that in 2015, Congress passed the Cybersecurity Information Sharing Act of 2015 (CISA) to authorize companies to monitor and implement defensive measures on their information systems, and to foreclose liability for such monitoring under CISA. AUTOMATED INDICATOR SHARING, https://www.us-cert.gov/ais (last visited Oct. 5, 2018); *See also* National Cyber Security Centre "Ten Steps to Cyber Security" [Step 8: Monitoring] (Aug. 9, 2016), https://www.ncsc.gov.uk/guidance/10-steps-cyber-security.
[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (2017).

intrusion despite reasonable or even extraordinary efforts by the lawyer. Thus, as is more fully explained below, the potential for an ethical violation occurs when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach.

2. Stopping the Breach and Restoring Systems

When a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach. How a lawyer does so in any particular circumstance is beyond the scope of this opinion. As a matter of preparation and best practices, however, lawyers should consider proactively developing an incident response plan with specific plans and procedures for responding to a data breach.[18] The decision whether to adopt a plan, the content of any plan, and actions taken to train and prepare for implementation of the plan, should be made before a lawyer is swept up in an actual breach. "One of the benefits of having an incident response capability is that it supports responding to incidents systematically (i.e., following a consistent incident handling methodology) so that the appropriate actions are taken. Incident response plans help personnel to minimize loss or theft of information and disruption of services caused by incidents."[19] While every lawyer's response plan should be tailored to the lawyer's or the law firm's specific practice, as a general matter incident response plans share common features:

> The primary goal of any incident response plan is to have a process in place that will allow the firm to promptly respond in a coordinated manner to any type of security incident or cyber intrusion. The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.
>
> Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported, and

[18] *See* ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 202 (explaining the utility of large law firms adopting "an incident response plan that details who has ownership of key decisions and the process to follow in the event of an incident.").

[19] *NIST Computer Security Incident Handling Guide*, at 6 (2012), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

> define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, as well as the team member charged with overall responsibility for the response.[20]

Whether or not the lawyer impacted by a data breach has an incident response plan in place, after taking prompt action to stop the breach, a competent lawyer must make all reasonable efforts to restore computer operations to be able again to service the needs of the lawyer's clients. The lawyer may do so either on her own, if qualified, or through association with experts. This restoration process provides the lawyer with an opportunity to evaluate what occurred and how to prevent a reoccurrence consistent with the obligation under Model Rule 1.6(c) that lawyers "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client."[21] These reasonable efforts could include (i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it, depending on the circumstances.

3. Determining What Occurred

The Model Rules do not impose greater or different obligations on a lawyer as a result of a breach involving client information, regardless of whether the breach occurs through electronic or physical means. Just as a lawyer would need to assess which paper files were stolen from the lawyer's office, so too lawyers must make reasonable attempts to determine whether electronic files were accessed, and if so, which ones. A competent attorney must make reasonable efforts to determine what occurred during the data breach. A post-breach investigation requires that the lawyer gather sufficient information to ensure the intrusion has been stopped and then, to the extent reasonably possible, evaluate the data lost or accessed. The information gathered in a post-breach investigation is necessary to understand the scope of the intrusion and to allow for accurate disclosure to the client consistent with the lawyer's duty of communication and honesty under

[20] Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, THE PROF'L LAWYER, Vol. 24, No. 3 (Nov. 2017).

[21] We discuss Model Rule 1.6(c) further below. But in restoring computer operations, lawyers should consider whether the lawyer's computer systems need to be upgraded or otherwise modified to address vulnerabilities, and further, whether some information is too sensitive to continue to be stored electronically.

Model Rules 1.4 and 8.4(c).[22] Again, how a lawyer actually makes this determination is beyond the scope of this opinion. Such protocols may be a part of an incident response plan.

B. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the Rule and the commentary about a lawyer's efforts that are required to preserve the confidentiality of information relating to the representation of a client. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.[23] The 2012 modification added a duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[24]

Amended Comment [18] explains:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. *See* Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and

[22] The rules against dishonesty and deceit may apply, for example, where the lawyer's failure to make an adequate disclosure --- or any disclosure at all --- amounts to deceit by silence. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.1 cmt. [1] (2018) ("Misrepresentations can also occur by partially true but misleading statements or omissions that are the equivalent of affirmative false statements.").

[23] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2018).

[24] *Id.* at (c).

- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[25]

As this Committee recognized in ABA Formal Opinion 477R:

> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors.

As discussed above and in Formal Opinion 477R, an attorney's competence in preserving a client's confidentiality is not a strict liability standard and does not require the lawyer to be invulnerable or impenetrable.[26] Rather, the obligation is one of reasonable efforts. Rule 1.6 is not violated even if data is lost or accessed if the lawyer has made reasonable efforts to prevent the loss or access.[27] As noted above, this obligation includes efforts to monitor for breaches of client confidentiality. The nature and scope of this standard is addressed in the ABA Cybersecurity Handbook:

> Although security is relative, a legal standard for "reasonable" security is emerging. That standard rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments.[28]

[25] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2018). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 9, at 5.

[26] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 122.

[27] MODEL RULES OF PROF'L CONDUCT R. 1.6, cmt. [18] (2018) ("The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.")

[28] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 73.

Finally, Model Rule 1.6 permits a lawyer to reveal information relating to the representation of a client if the disclosure is impliedly authorized in order to carry out the representation. Such disclosures are permitted if the lawyer reasonably believes that disclosure: (1) is impliedly authorized and will advance the interests of the client in the representation, and (2) will not affect a material interest of the client adversely.[29] In exercising this discretion to disclose information to law enforcement about the data breach, the lawyer must consider: (i) whether the client would object to the disclosure; (ii) whether the client would be harmed by the disclosure; and (iii) whether reporting the theft would benefit the client by assisting in ending the breach or recovering stolen information. Even then, without consent, the lawyer may disclose only such information as is reasonably necessary to assist in stopping the breach or recovering the stolen information.

C. Lawyer's Obligations to Provide Notice of Data Breach

When a lawyer knows or reasonably should know a data breach has occurred, the lawyer must evaluate notice obligations. Due to record retention requirements of Model Rule 1.15, information compromised by the data breach may belong or relate to the representation of a current client or former client.[30] We address each below.

1. Current Client

Communications between a lawyer and current client are addressed generally in Model Rule 1.4. Rule 1.4(a)(3) provides that a lawyer must "keep the client reasonably informed about the status of the matter." Rule 1.4(b) provides: "A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation." Under these provisions, an obligation exists for a lawyer to communicate with current clients about a data breach.[31]

[29] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 01-421(2001) (disclosures to insurer in bills when lawyer representing insured).

[30] This opinion addresses only obligations to clients and former clients. Data breach, as used in this opinion, is limited to client confidential information. We do not address ethical duties, if any, to third parties.

[31] Relying on Rule 1.4 generally, the New York State Bar Committee on Professional Ethics concluded that a lawyer must notify affected clients of information lost through an online data storage provider. N.Y. State Bar Ass'n Op. 842 (2010) (Question 10: "If the lawyer learns of any breach of confidentiality by the online storage provider, then the lawyer must investigate whether there has been any breach of his or her own clients' confidential information,

Our conclusion here is consistent with ABA Formal Ethics Opinion 95-398 where this Committee said that notice must be given to clients if a breach of confidentiality was committed by or through a third-party computer vendor or other service provider. There, the Committee concluded notice to the client of the breach may be required under 1.4(b) for a "serious breach."[32] The Committee advised:

> Where the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b).[33]

A data breach under this opinion involves the misappropriation, destruction or compromise of client confidential information, or a situation where a lawyer's ability to perform the legal services for which the lawyer was hired is significantly impaired by the event. Each of these scenarios is one where a client's interests have a reasonable possibility of being negatively impacted. When a data breach occurs involving, or having a substantial likelihood of involving, material client confidential information a lawyer has a duty to notify the client of the breach. As noted in ABA Formal Opinion 95-398, a data breach requires notice to the client because such notice is an integral part of keeping a "client reasonably informed about the status of the matter" and the lawyer should provide information as would be "reasonably necessary to permit the client to make informed decisions regarding the representation" within the meaning of Model Rule 1.4.[34]

The strong client protections mandated by Model Rule 1.1, 1.6, 5.1 and 5.3, particularly as they were amended in 2012 to account for risks associated with the use of technology, would be compromised if a lawyer who experiences a data breach that impacts client confidential information is permitted to hide those events from their clients. And in view of the duties imposed by these other Model Rules, Model Rule 1.4's requirement to keep clients "reasonably informed about the status" of a matter would ring hollow if a data breach was somehow excepted from this responsibility to communicate.

notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.") (*citations omitted*).

[32] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

[33] *Id.*

[34] MODEL RULES OF PROF'L CONDUCT R. 1.4(b) (2018).

Model Rule 1.15(a) provides that a lawyer shall hold "property" of clients "in connection with a representation separate from the lawyer's own property." Funds must be kept in a separate account, and "[o]ther property shall be identified as such and appropriately safeguarded." Model Rule 1.15(a) also provides that, "Complete records of such account funds and other property shall be kept by the lawyer . . . ." Comment [1] to Model Rule 1.15 states:

> A lawyer should hold property of others with the care required of a professional fiduciary. Securities should be kept in a safe deposit box, except when some other form of safekeeping is warranted by special circumstances. All property that is the property of clients or third persons, including prospective clients, must be kept separate from the lawyer's business and personal property.

An open question exists whether Model Rule 1.15's reference to "property" includes information stored in electronic form. Comment [1] uses as examples "securities" and "property" that should be kept separate from the lawyer's "business and personal property." That language suggests Rule 1.15 is limited to tangible property which can be physically segregated. On the other hand, many courts have moved to electronic filing and law firms routinely use email and electronic document formats to image or transfer information. Reading Rule 1.15's safeguarding obligation to apply to hard copy client files but not electronic client files is not a reasonable reading of the Rule.

Jurisdictions that have addressed the issue are in agreement. For example, Arizona Ethics Opinion 07-02 concluded that client files may be maintained in electronic form, with client consent, but that lawyers must take reasonable precautions to safeguard the data under the duty imposed in Rule 1.15. The District of Columbia Formal Ethics Opinion 357 concluded that, "Lawyers who maintain client records solely in electronic form should take reasonable steps (1) to ensure the continued availability of the electronic records in an accessible form during the period for which they must be retained and (2) to guard against the risk of unauthorized disclosure of client information."

The Committee has engaged in considerable discussion over whether Model Rule 1.15 and, taken together, the technology amendments to Rules 1.1, 1.6, and 5.3 impliedly impose an obligation on a lawyer to notify a current client of a data breach. We do not have to decide that question in the absence of concrete facts. We reiterate, however, the obligation to inform the client does exist under Model Rule 1.4.

2. Former Client

Model Rule 1.9(c) requires that "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 . . . reveal information relating to the representation except as these Rules would permit or require with respect to a client."[35] When electronic "information relating to the representation" of a former client is subject to unauthorized access, disclosure, or destruction, the Model Rules provide no direct guidance on a lawyer's obligation to notify the former client. Rule 1.9(c) provides that a lawyer "shall not . . . reveal" the former client's information. It does not describe what steps, if any, a lawyer should take if such information is revealed. The Committee is unwilling to require notice to a former client as a matter of legal ethics in the absence of a black letter provision requiring such notice.[36]

Nevertheless, we note that clients can make an informed waiver of the protections in Rule 1.9.[37] We also note that Rule 1.16(d) directs that lawyers should return "papers and property" to clients at the conclusion of the representation, which has commonly been understood to include the client's file, in whatever form it is held. Rule 1.16(d) also has been interpreted as permitting lawyers to establish appropriate data destruction policies to avoid retaining client files and property indefinitely.[38] Therefore, as a matter of best practices, lawyers are encouraged to reach agreement with clients before conclusion, or at the termination, of the relationship about how to handle the client's electronic information that is in the lawyer's possession.

Absent an agreement with the former client lawyers are encouraged to adopt and follow a paper and electronic document retention schedule, which meets all applicable laws and rules, to reduce the amount of information relating to the representation of former clients that the lawyers retain. In addition, lawyers should recognize that in the event of a data breach involving former client information, data privacy laws, common law duties of care, or contractual arrangements with

[35] MODEL RULES OF PROF'L CONDUCT R. 1.9(c)(2) (2018).

[36] *See* Discipline of Feland, 2012 ND 174, ¶ 19, 820 N.W.2d 672 (Rejecting respondent's argument that the court should engraft an additional element of proof in a disciplinary charge because "such a result would go beyond the clear language of the rule and constitute amendatory rulemaking within an ongoing disciplinary proceeding.").

[37] *See* MODEL RULES OF PROF'L CONDUCT R. 1.9, cmt. [9] (2018).

[38] *See* ABA Ethics Search Materials on Client File Retention, https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/piles_of_files_2008.pdf (last visited Oct.15, 2018).

the former client relating to records retention, may mandate notice to former clients of a data breach. A prudent lawyer will consider such issues in evaluating the response to the data breach in relation to former clients.[39]

3. Breach Notification Requirements

The nature and extent of the lawyer's communication will depend on the type of breach that occurs and the nature of the data compromised by the breach. Unlike the "safe harbor" provisions of Comment [18] to Model Rule 1.6, if a post-breach obligation to notify is triggered, a lawyer must make the disclosure irrespective of what type of security efforts were implemented prior to the breach. For example, no notification is required if the lawyer's office file server was subject to a ransomware attack but no information relating to the representation of a client was inaccessible for any material amount of time, or was not accessed by or disclosed to unauthorized persons. Conversely, disclosure will be required if material client information was actually or reasonably suspected to have been accessed, disclosed or lost in a breach.

The disclosure must be sufficient to provide enough information for the client to make an informed decision as to what to do next, if anything. In a data breach scenario, the minimum disclosure required to all affected clients under Rule 1.4 is that there has been unauthorized access to or disclosure of their information, or that unauthorized access or disclosure is reasonably suspected of having occurred. Lawyers must advise clients of the known or reasonably ascertainable extent to which client information was accessed or disclosed. If the lawyer has made reasonable efforts to ascertain the extent of information affected by the breach but cannot do so, the client must be advised of that fact.

In addition, and as a matter of best practices, a lawyer also should inform the client of the lawyer's plan to respond to the data breach, from efforts to recover information (if feasible) to steps being taken to increase data security.

The Committee concludes that lawyers have a continuing duty to keep clients reasonably apprised of material developments in post-breach investigations affecting the clients'

[39] *Cf.* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 482 (2018), at 8-10 (discussing obligations regarding client files lost or destroyed during disasters like hurricanes, floods, tornadoes, and fires).

information.[40] Again, specific advice on the nature and extent of follow up communications cannot be provided in this opinion due to the infinite number of variable scenarios.

If personally identifiable information of clients or others is compromised as a result of a data beach, the lawyer should evaluate the lawyer's obligations under state and federal law. All fifty states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have statutory breach notification laws.[41] Those statutes require that private or governmental entities notify individuals of breaches involving loss or disclosure of personally identifiable information.[42] Most breach notification laws specify who must comply with the law, define "personal information," define what constitutes a breach, and provide requirements for notice.[43] Many federal and state agencies also have confidentiality and breach notification requirements.[44] These regulatory schemes have the potential to cover individuals who meet particular statutory notice triggers, irrespective of the individual's relationship with the lawyer. Thus, beyond a Rule 1.4 obligation, lawyers should evaluate whether they must provide a statutory or regulatory data breach notification to clients or others based upon the nature of the information in the lawyer's possession that was accessed by an unauthorized user.[45]

III. Conclusion

Even lawyers who, (i) under Model Rule 1.6(c), make "reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," (ii) under Model Rule 1.1, stay abreast of changes in technology, and (iii) under Model Rules 5.1 and 5.3, properly supervise other lawyers and third-party electronic-information storage vendors, may suffer a data breach. When they do, they have a duty to notify clients of the data

[40] State Bar of Mich. Op. RI-09 (1991).
[41] National Conference of State Legislatures, *Security Breach Notification Laws* (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[42] *Id.*
[43] *Id.*
[44] ABA CYBERSECURITY HANDBOOK, *supra* note 11, at 65.
[45] Given the broad scope of statutory duties to notify, lawyers would be well served to actively manage the amount of confidential and or personally identifiable information they store beyond any ethical, statutory, or other legal obligation to do so. Lawyers should implement, and follow, a document retention policy that comports with Model Rule 1.15 and evaluate ways to limit receipt, possession and/or retention of confidential or personally identifiable information during or after an engagement.

breach under Model Rule 1.4 in sufficient detail to keep clients "reasonably informed" and with an explanation "to the extent necessary to permit the client to make informed decisions regarding the representation."

AMERICAN BAR ASSOCIATION

STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

Formal Opinion 477R* **May 11, 2017**

Revised May 22, 2017

Securing Communication of Protected Client Information

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

I. Introduction

In Formal Opinion 99-413 this Committee addressed a lawyer's confidentiality obligations for email communications with clients. While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved since 1999 prompting the need to update Opinion 99-413.

Formal Opinion 99-413 concluded: "Lawyers have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure. It therefore follows that its use is consistent with the duty under Rule 1.6 to use reasonable means to maintain the confidentiality of information relating to a client's representation."[1]

Unlike 1999 where multiple methods of communication were prevalent, today, many lawyers primarily use electronic means to communicate and exchange documents with clients, other lawyers, and even with other persons who are assisting a lawyer in delivering legal services to clients.[2]

Since 1999, those providing legal services now regularly use a variety of devices to create, transmit and store confidential communications, including desktop, laptop and notebook

*The opinion below is a revision of, and replaces Formal Opinion 477 as issued by the Committee May 11, 2017. This opinion is based on the ABA Model Rules of Professional Conduct as amended by the ABA House of Delegates through August 2016. The laws, court rules, regulations, rules of professional conduct, and opinions promulgated in individual jurisdictions are controlling.

[1] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, at 11 (1999).

[2] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008); ABA COMMISSION ON ETHICS 20/20 REPORT TO THE HOUSE OF DELEGATES (2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_resolution_and_report_outsourcing_posting.authcheckdam.pdf.

computers, tablet devices, smartphones, and cloud resource and storage locations. Each device and each storage location offer an opportunity for the inadvertent or unauthorized disclosure of information relating to the representation, and thus implicate a lawyer's ethical duties.[3]

In 2012 the ABA adopted "technology amendments" to the Model Rules, including updating the Comments to Rule 1.1 on lawyer technological competency and adding paragraph (c) and a new Comment to Rule 1.6, addressing a lawyer's obligation to take reasonable measures to prevent inadvertent or unauthorized disclosure of information relating to the representation.

At the same time, the term "cybersecurity" has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the internet. Cybersecurity recognizes a post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of "when," and not "if."[4] Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client.[5]

The Model Rules do not impose greater or different duties of confidentiality based upon the method by which a lawyer communicates with a client. But how a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection.

Against this backdrop we describe the "technology amendments" made to the Model Rules in 2012, identify some of the technology risks lawyers face, and discuss factors other than the Model Rules of Professional Conduct that lawyers should consider when using electronic means to communicate regarding client matters.

II. Duty of Competence

Since 1983, Model Rule 1.1 has read: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[6] The scope of this requirement was

[3] *See* JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 7 (2013) [hereinafter ABA CYBERSECURITY HANDBOOK].

[4] "Cybersecurity" is defined as "measures taken to protect a computer or computer system (as on the internet) against unauthorized access or attack." CYBERSECURITY, MERRIAM WEBSTER, http://www.merriam-webster.com/dictionary/cybersecurity (last visited Sept. 10, 2016). In 2012 the ABA created the Cybersecurity Legal Task Force to help lawyers grapple with the legal challenges created by cyberspace. In 2013 the Task Force published The ABA Cybersecurity Handbook: A Resource For Attorneys, Law Firms, and Business Professionals.

[5] Bradford A. Bleier, Unit Chief to the Cyber National Security Section in the FBI's Cyber Division, indicated that "[l]aw firms have tremendous concentrations of really critical private information, and breaking into a firm's computer system is a really optimal way to obtain economic and personal security information." Ed Finkel, Cyberspace Under Siege, A.B.A. J., Nov. 1, 2010.

[6] A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2013, at 37-44 (Art Garwin ed., 2013).

clarified in 2012 when the ABA recognized the increasing impact of technology on the practice of law and the duty of lawyers to develop an understanding of that technology. Thus, Comment [8] to Rule 1.1 was modified to read:

> 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. (Emphasis added.)[7]

Regarding the change to Rule 1.1's Comment, the ABA Commission on Ethics 20/20 explained:

> Model Rule 1.1 requires a lawyer to provide competent representation, and Comment [6] [renumbered as Comment [8]] specifies that, to remain competent, lawyers need to "keep abreast of changes in the law and its practice." The Commission concluded that, in order to keep abreast of changes in law practice in a digital age, lawyers necessarily need to understand basic features of relevant technology and that this aspect of competence should be expressed in the Comment. For example, a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document. [8]

III. Duty of Confidentiality

In 2012, amendments to Rule 1.6 modified both the rule and the commentary about what efforts are required to preserve the confidentiality of information relating to the representation. Model Rule 1.6(a) requires that "A lawyer shall not reveal information relating to the representation of a client" unless certain circumstances arise.[9] The 2012 modification added a new duty in paragraph (c) that: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[10]

[7] *Id.* at 43.

[8] ABA COMMISSION ON ETHICS 20/20 REPORT 105A (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf. The 20/20 Commission also noted that modification of Comment [6] did not change the lawyer's substantive duty of competence: "Comment [6] already encompasses an obligation to remain aware of changes in technology that affect law practice, but the Commission concluded that making this explicit, by addition of the phrase 'including the benefits and risks associated with relevant technology,' would offer greater clarity in this area and emphasize the importance of technology to modern law practice. The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent."

[9] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2016).

[10] *Id.* at (c).

Amended Comment [18] explains:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.[11]

Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

> . . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.[12]

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,

[11] The 20/20 Commission's report emphasized that lawyers are not the guarantors of data safety. It wrote: "[t]o be clear, paragraph (c) does not mean that a lawyer engages in professional misconduct any time a client's confidences are subject to unauthorized access or disclosed inadvertently or without authority. A sentence in Comment [16] makes this point explicitly. The reality is that disclosures can occur even if lawyers take all reasonable precautions. The Commission, however, believes that it is important to state in the black letter of Model Rule 1.6 that lawyers have a duty to take reasonable precautions, even if those precautions will not guarantee the protection of confidential information under all circumstances."

[12] ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 48-49.

- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[13]

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures.[14] Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

[13] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. [18] (2016). "The [Ethics 20/20] Commission examined the possibility of offering more detailed guidance about the measures that lawyers should employ. The Commission concluded, however, that technology is changing too rapidly to offer such guidance and that the particular measures lawyers should use will necessarily change as technology evolves and as new risks emerge and new security procedures become available." ABA COMMISSION REPORT 105A, *supra* note 8, at 5.

[14] See item 3 below.

While it is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts, we offer the following considerations as guidance:

1. Understand the Nature of the Threat.

   Understanding the nature of the threat includes consideration of the sensitivity of a client's information and whether the client's matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft.[15] "Reasonable efforts" in higher risk scenarios generally means that greater effort is warranted.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

   A lawyer should understand how their firm's electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer's task is complicated in a world where multiple devices may be used to communicate with or about a client and then store those communications. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures.

   Model Rule 1.6(c) requires a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client. As Comment [18] makes clear, what is deemed to be "reasonable" may vary, depending on the facts and circumstances of each case. Electronic disclosure of, or access to, client communications can occur in different forms ranging from a direct intrusion into a law firm's systems to theft or interception of information during the transmission process. Making reasonable efforts to protect against unauthorized disclosure in client communications thus includes analysis of security measures applied to both disclosure and access to a law firm's technology system and transmissions.

   A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique complex

[15] *See, e.g.,* Noah Garner, *The Most Prominent Cyber Threats Faced by High-Target Industries,* TREND-MICRO (Jan. 25, 2016), http://blog.trendmicro.com/the-most-prominent-cyber-threats-faced-by-high-target-industries/.

passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used.

Other available tools include encryption of data that is physically stored on a device and multi-factor authentication to access firm systems.

In the electronic world, "delete" usually does not mean information is permanently deleted, and "deleted" data may be subject to recovery. Therefore, a lawyer should consider whether certain data should *ever* be stored in an unencrypted environment, or electronically transmitted at all.

4. Determine How Electronic Communications About Clients Matters Should Be Protected.

Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer should encrypt the transmission and determine how to do so to sufficiently protect it,[16] and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

Thus, routine communications sent electronically are those communications that do not contain information warranting additional security measures beyond basic methods. However, in some circumstances, a client's lack of technological sophistication or the limitations of technology available to the client may require alternative non-electronic forms of communication altogether.

[16] *See* Cal. Formal Op. 2010-179 (2010); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 121. Indeed, certain laws and regulations require encryption in certain situations. *Id.* at 58-59.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party.[17] If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived. Therefore, the lawyer should warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.[18]

5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as "privileged and confidential" in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or "disclaimer" to client emails, where such a disclaimer is accurate and appropriate for the communication.[19]

Model Rule 4.4(b) obligates a lawyer who "knows or reasonably should know" that he has received an inadvertently sent "document or electronically stored information relating to the representation of the lawyer's client" to promptly notify the sending lawyer. A clear and conspicuous appropriately used disclaimer may affect whether a recipient lawyer's duty under Model Rule 4.4(b) for inadvertently transmitted communications is satisfied.

[17] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459, Duty to Protect the Confidentiality of E-mail Communications with One's Client (2011). Formal Op. 11-459 was issued prior to the 2012 amendments to Rule 1.6. These amendments added new Rule 1.6(c), which provides that lawyers "shall" make reasonable efforts to prevent the unauthorized or inadvertent access to client information. *See, e.g.,* Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04-CV-139-RJC-DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (employee communications with lawyer over company owned computer not privileged); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases on privilege waiver for privileged emails sent or received through an employer's email server).

[18] Some state bar ethics opinions have explored the circumstances under which email communications should be afforded special security protections. *See, e.g.*, Tex. Prof'l Ethics Comm. Op. 648 (2015) that identified six situations in which a lawyer should consider whether to encrypt or use some other type of security precaution:

- communicating highly sensitive or confidential information via email or unencrypted email connections;
- sending an email to or from an account that the email sender or recipient shares with others;
- sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer…;
- sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
- sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
- sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

[19] *See* Veteran Med. Prods. v. Bionix Dev. Corp., Case No. 1:05-cv-655, 2008 WL 696546 at *8, 2008 BL 51876 at *8 (W.D. Mich. Mar. 13, 2008) (email disclaimer that read "this email and any files transmitted with are confidential and are intended solely for the use of the individual or entity to whom they are addressed" with nondisclosure constitutes a reasonable effort to maintain the secrecy of its business plan).

6. Train Lawyers and Nonlawyer Assistants in Technology and Information Security.

Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct. Model Rule 5.1 also provides that lawyers having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct. In addition, Rule 5.3 requires lawyers who are responsible for managing and supervising nonlawyer assistants to take reasonable steps to reasonably assure that the conduct of such assistants is compatible with the ethical duties of the lawyer. These requirements are as applicable to electronic practices as they are to comparable office procedures.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.

Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

In ABA Formal Opinion 08-451, this Committee analyzed Model Rule 5.3 and a lawyer’s obligation when outsourcing legal and nonlegal services. That opinion identified several issues a lawyer should consider when selecting the outsource vendor, to meet the lawyer’s due diligence and duty of supervision. Those factors also apply in the analysis of vendor selection in the context of electronic communications. Such factors may include:

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and

- the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.[20]

Since the issuance of Formal Opinion 08-451, Comment [3] to Model Rule 5.3 was added to address outsourcing, including "using an Internet-based service to store client information." Comment [3] provides that the "reasonable efforts" required by Model Rule 5.3 to ensure that the nonlawyer's services are provided in a manner that is compatible with the lawyer's professional obligations "will depend upon the circumstances." Comment [3] contains suggested factors that might be taken into account:

- the education, experience, and reputation of the nonlawyer;
- the nature of the services involved;
- the terms of any arrangements concerning the protection of client information; and
- the legal and ethical environments of the jurisdictions in which the services will be performed particularly with regard to confidentiality.

Comment [3] further provides that when retaining or directing a nonlawyer outside of the firm, lawyers should communicate "directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer."[21] If the client has not directed the selection of the outside nonlawyer vendor, the lawyer has the responsibility to monitor how those services are being performed.[22]

Even after a lawyer examines these various considerations and is satisfied that the security employed is sufficient to comply with the duty of confidentiality, the lawyer must periodically reassess these factors to confirm that the lawyer's actions continue to comply with the ethical obligations and have not been rendered inadequate by changes in circumstances or technology.

[20] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmts. [2] & [8] (2016).

[21] The ABA's catalog of state bar ethics opinions applying the rules of professional conduct to cloud storage arrangements involving client information can be found at: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

[22] By contrast, where a client directs the selection of a particular nonlawyer service provider outside the firm, "the lawyer ordinarily should agree with the client concerning the allocation of responsibility for monitoring as between the client and the lawyer." MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. [4] (2016). The concept of monitoring recognizes that although it may not be possible to "directly supervise" a client directed nonlawyer outside the firm performing services in connection with a matter, a lawyer must nevertheless remain aware of how the nonlawyer services are being performed. ABA COMMISSION ON ETHICS 20/20 REPORT 105C, at 12 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105c_filed_may_2012.authcheckdam.pdf.

IV. Duty to Communicate

Communications between a lawyer and client generally are addressed in Rule 1.4. When the lawyer reasonably believes that highly sensitive confidential client information is being transmitted so that extra measures to protect the email transmission are warranted, the lawyer should inform the client about the risks involved.[23] The lawyer and client then should decide whether another mode of transmission, such as high level encryption or personal delivery is warranted. Similarly, a lawyer should consult with the client as to how to appropriately and safely use technology in their communication, in compliance with other laws that might be applicable to the client. Whether a lawyer is using methods and practices to comply with administrative, statutory, or international legal standards is beyond the scope of this opinion.

A client may insist or require that the lawyer undertake certain forms of communication. As explained in Comment [19] to Model Rule 1.6, "A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule."

V. Conclusion

Rule 1.1 requires a lawyer to provide competent representation to a client. Comment [8] to Rule 1.1 advises lawyers that to maintain the requisite knowledge and skill for competent representation, a lawyer should keep abreast of the benefits and risks associated with relevant technology. Rule 1.6(c) requires a lawyer to make "reasonable efforts" to prevent the inadvertent or unauthorized disclosure of or access to information relating to the representation.

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

AMERICAN BAR ASSOCIATION STANDING COMMITTEE ON ETHICS AND PROFESSIONAL RESPONSIBILITY

321 N. Clark Street, Chicago, Illinois 60654-4714 Telephone (312) 988-5328

[23] MODEL RULES OF PROF'L CONDUCT R. 1.4(a)(1) & (4) (2016).

John Bandler, Contributor
Founder of Bandler Law Firm PLLC and Bandler Group LLC

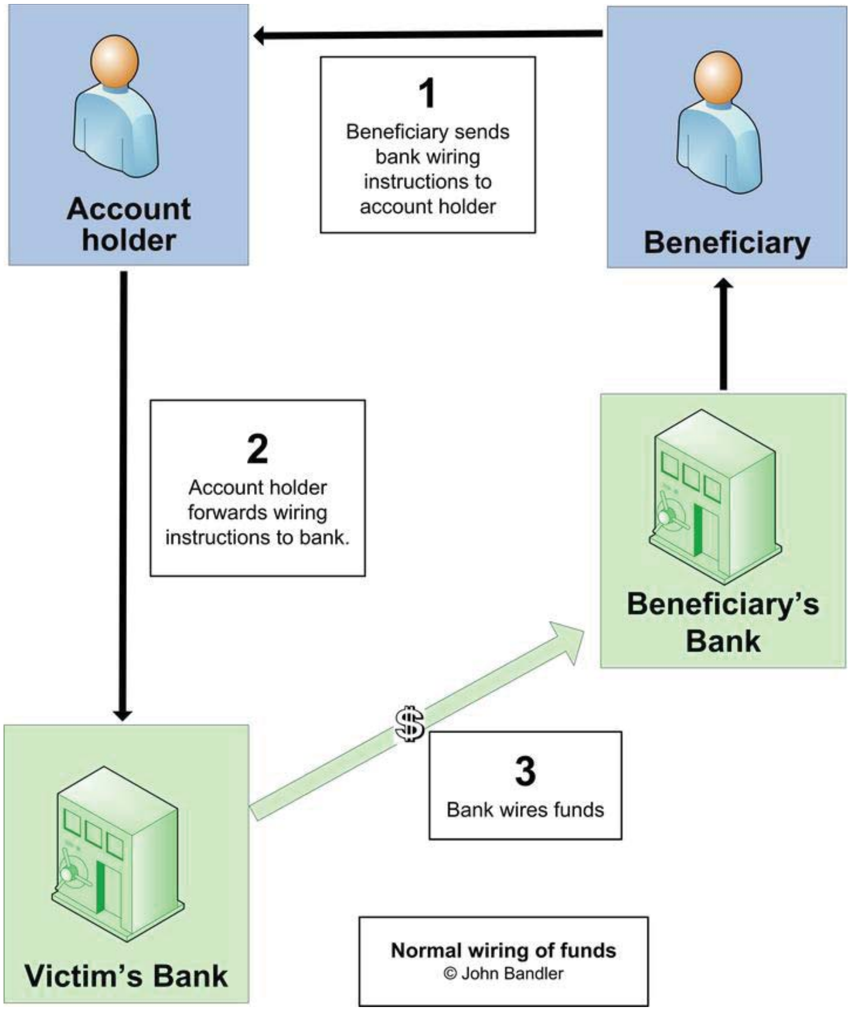
The Cybercrime Scheme That Attacks Email Accounts And Your Bank Accounts

08/03/2017 01:49 pm ET | **Updated** Aug 03, 2017

Cybercrime is ever present, and there is one particular fraud we all should be aware of -- particularly anyone who sends or receives bank wiring instructions or the funds themselves. The fraud involves the hacking or impersonating of email accounts, it might be called business email compromise (BEC) fraud, CEO fraud, or CFO fraud, and it demonstrates that criminal participants are infinitely adaptable in pursuit of profitable schemes. Cybercrime is not always a technical attack, but often about social engineering -- tricking a person into performing an action -- which means we need to stay informed, be alert, and exercise sound judgement.

Email schemes and bank wiring frauds

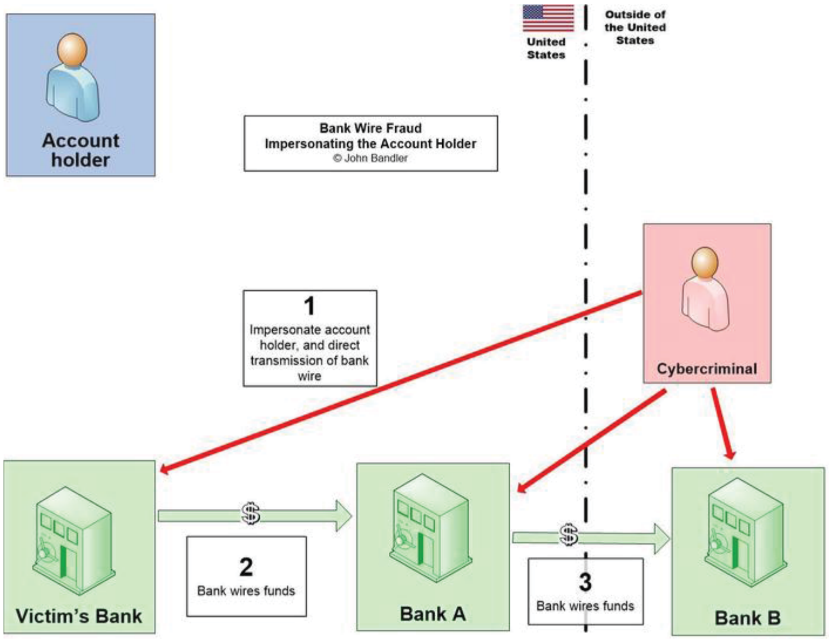
First, let's review how things are *supposed* to work when we send a bank wire. We want to send money from our bank account to theirs, the recipient tells us where we should wire the funds, we relay those instructions to the bank, and the bank sends the money from our account to the beneficiary's account.


Account holder
1
Beneficiary sends bank wiring instructions to account holder
Beneficiary
2
Account holder forwards wiring instructions to bank.
Beneficiary's Bank
$
3
Bank wires funds
Victim's Bank
Normal wiring of funds
© John Bandler

JOHN BANDLER

Normal wiring of funds

When cybercrime was a newer industry, cybercriminals attacked banks who then learned to protect themselves. Then cybercriminals realized that the account holder was an easier point of compromise, with less security than the bank. By compromising the account holder's financial account credentials, or email account credentials, they could impersonate the account holder, direct the bank to send a wire to an account controlled by the criminal, and then forward the funds out of the country. This was done without the consent or knowledge of the account holder, and is depicted like this.

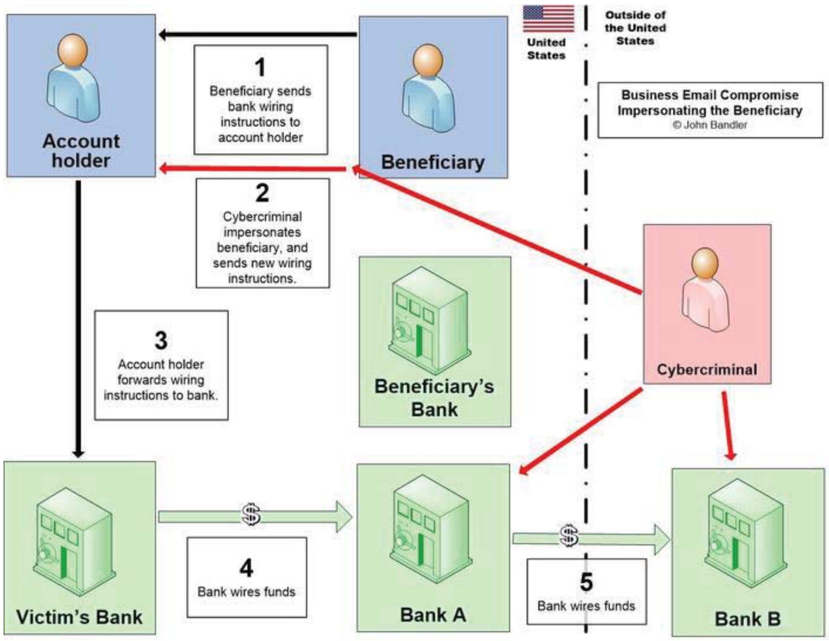


JOHN BANDLER

Bank Wire Fraud - Impersonating the Account Holder

When this scheme is successful the criminals get away scot-free with the money, and then it is between the account holder and bank to figure out who should bear the loss. Sometimes fault is not clear, but if the account holder was negligent in allowing their internet account or computer to be hacked, perhaps they should bear some or all of the loss. If the bank was tricked by a criminal, and wired customer funds without the consent of the account holder, then perhaps the bank should bear the entire loss. The result was that banks became wise to this fraud and implemented controls to reduce it, taking steps to confirm that the wiring instructions are being sent by the account holder—and not by a fraudster. These measures include a verbal conversation and confirmation of bank wiring instructions. While anti-fraud measures are good business practices and protect against monetary loss, banks also have legal and regulatory obligations to prevent and report fraud and money laundering activity, and are in an excellent position to identify and respond to new fraud trends.

With these improved controls it became harder for cybercriminals to commit that specific fraud so they evolved. Instead of impersonating the account holder and tricking the bank, they impersonate the person who sends the account holder the bank wiring instructions—tricking the account holder. Unlike the bank, the account holder probably has no training in anti-fraud and anti-money laundering, and may not know about the need to verify that wiring instructions are authentic. The account holder receives fraudulent instructions and simply forwards them to the bank. The bank receives these instructions from the account holder, and verifies that the instructions were in fact sent from the account holder, but perhaps does nothing to advise the account holder about this new fraud scheme. The bank executes the customer's instructions, the money is wired, and thus stolen, as shown below.


United States
Outside of the United States
Business Email Compromise
Impersonating the Beneficiary
© John Bandler
Account holder
Beneficiary
1
Beneficiary sends bank wiring instructions to account holder
2
Cybercriminal impersonates beneficiary, and sends new wiring instructions.
Cybercriminal
3
Account holder forwards wiring instructions to bank.
Beneficiary's Bank
Victim's Bank
4
Bank wires funds
Bank A
5
Bank wires funds
Bank B

JOHN BANDLER

Impersonating the Beneficiary

This fraud is rampant, and many banks take the position that this is solely the fault of the account holder, who must bear the entire theft loss, given that the bank merely did what the account holder instructed it to do. Some banks seem to expend minimal effort to recover the stolen funds, especially in the critical hours after the first wire transfer. However, it is the banks who are in the best position to move quickly, trace the funds, and stop them from moving further, especially before they are transferred out of the country. It is also the banks who are in the best position to identify money mule accounts, as the account in “Bank A” represents. Arguably, banks might act more aggressively to recover stolen funds if it were *their* funds to be recovered, rather than their customer’s funds, and there are probably instances where the bank may not be as blameless nor as diligent as it might lead the customer to believe.

The money mule

The cybercriminals committing this fraud don’t receive stolen funds directly, so they use one or more money mules—people recruited to receive a fraudulent bank wire or forged check—to receive and then forward the funds. The cybercrime economy is lucrative, so it is now very good at laundering money, and this is one way they do it.

Cybercriminals use a variety of techniques to recruit money mules to receive these fraudulent bank wires or forged checks. A fraudster tried to recruit me the other day with this email:

> *Hi, Can you help us in drafting a purchase … agreement of oil rig equipment with a buyer in your state?*
>
> *Regards,*
>
> *[Impersonated victim's name]*

Had I responded, eventually they would have asked me to receive a check or a bank wire which would eventually be revealed as fraudulent. This solicitation wasn't believable—especially since New York isn't a big market for buyers of oil rig equipment—but others are more believable. It could be "work at home" business opportunities to help collect a debt, settlement, or purchase property. The unsuspecting money mule thinks he or she will earn a fee for this service, but will earn nothing, and may face civil liability for the entire amount of the fraudulent transaction. Money mules are needed for frauds of all sizes, from hundreds of dollars to millions of dollars.

Protect yourself

There's a few things you need to do to protect yourself. They boil down to:

- Keep your financial and email accounts from being hacked.
- Verify that people you deal with haven't had their accounts hacked.
- Confirm wiring instructions verbally.
- Don't become a money mule. Know who you are dealing with, know their business, and know the source and destination of funds.

You can keep your email accounts and financial accounts from being hacked by using strong passwords that are changed periodically, and by enabling two factor authentication (two step login). Periodically review your privacy and security settings.

Ensure that you—and your company—always verbally confirm payment instructions that are sent to you from people inside or outside your organization. Businesses also need financial controls which include dual control and segregation of duties to prevent a single person from causing funds to be sent. Get to know the people and businesses that you work with and transfer funds with. If things seem suspicious, or change without adequate explanation and confirmation, or if names don't match, that could indicate fraud or money laundering.

If you are a victim

If you are a victim of this crime, report it to the bank and to law enforcement immediately. Report to the FBI's Internet Crime Complaint Center (IC3), report to the local police, and if the fraud amount is significant call the local FBI field office. See the FBI's advisory on this fraud for more information.

Preserve all evidence of the crime, and document your communications with the bank and law enforcement. Of course, preserve all communications to and from the cybercriminals, and don't delete those emails.

Consider hiring a professional to assist you. The bank's interests are different from yours and they may not be as motivated to recover funds if they believe it is your money, rather than theirs. Banks might not be allowed to share certain information with you by law, and sometimes they might not share information if it might be ammunition in a lawsuit or regulatory action. Law enforcement might not investigate as thoroughly as you might like, and even when they do, their focus is pursuing a criminal investigation, and they might not be allowed to share certain information with you.

In order to effectively fight cybercrime, our country will need to develop seamless crime reporting methods, which are followed by a prompt and effective investigative response. We are not there yet, so persistence by the crime victim may be required. We should encourage government to comprehensively fight the cybercrime economy, which it is not yet doing. This fraud is one of many evolving frauds, so personal and business cybersecurity and anti-fraud measures are

THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK
COMMITTEE ON PROFESSIONAL ETHICS

FORMAL OPINION 2017-5: An Attorney's Ethical Duties Regarding U.S. Border Searches of Electronic Devices Containing Clients' Confidential Information

TOPIC: Duty to protect clients' confidential information from disclosure that the client has not authorized; disclosure when border agents claiming lawful authority request access to clients' confidential information; obligations upon disclosing clients' confidential information.

DIGEST: Under the New York Rules of Professional Conduct (the "Rules"), a New York lawyer has certain ethical obligations when crossing the U.S. border with confidential client information. Before crossing the border, the Rules require a lawyer to take reasonable steps to avoid disclosing confidential information in the event a border agent seeks to search the attorney's electronic device. The "reasonableness" standard does not imply that particular protective measures must invariably be adopted in all circumstances to safeguard clients' confidential information; however, this opinion identifies measures that may satisfy the obligation to safeguard clients' confidences in this situation. Additionally, Under Rule 1.6(b)(6), the lawyer may not disclose a client's confidential information in response to a claim of lawful authority unless doing so is "reasonably necessary" to comply with a border agent's claim of lawful authority. This includes first making reasonable efforts to assert the attorney-client privilege and to otherwise avert or limit the disclosure of confidential information. Finally, if the attorney discloses clients' confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures pursuant to Rule 1.4.

RULES: 1.1, 1.4, 1.6

QUESTION: What are an attorney's ethical obligations with regard to the protection of confidential information prior to crossing a U.S. border, during border searches and thereafter?

OPINION:

I. Introduction

This opinion considers attorneys' ethical obligations in the context of the following scenario:

> An attorney traveling abroad with an electronic device (such as a smartphone, portable hard drive, USB "thumb drive," or laptop) that contains clients' confidential information plans to travel through a U.S. customs checkpoint or border crossing. During the crossing, a U.S. Customs and Border Protection ("CBP") agent claiming lawful authority demands that the attorney "unlock" the device and hand it to the agent so that it may be searched. The attorney has not

> obtained informed consent from each client whose information may be disclosed in this situation.[1]

Searches of electronic devices at the U.S. border when travelers enter or leave the U.S. may include not only a physical inspection of these devices but also the review of information stored on them, such as emails, text messages and electronically-stored documents.[2] CBP policy permits U.S. customs agents to review any information that physically resides on travelers' electronic devices, including those of U.S. citizens, with or without any reason for suspicion, to demand disclosure of social media and email account passwords, and to seize the devices pending an inspection.[3] In recent years, searches of cell phones, laptop computers, and other electronic devices at border crossings into the U.S. have become increasingly frequent. According to the Department of Homeland Security, more than 5,000 devices were searched by CBP agents in February 2017 alone. By way of comparison, that is about as many U.S. border searches of electronic devices as were undertaken in all of 2015, and just under a quarter of the approximately 23,877 U.S. border searches of such devices undertaken in 2016. Further, border agents have access to software tools that increase the effectiveness and thoroughness of device searches, and they have the ability to copy the contents of such devices to be reviewed later. To be sure, the 5000-plus individuals whose devices were searched in February 2017 amounted to only a fraction of the 1,069,266 individuals entering into the United States *daily* as reported by the CBP.[4] However, depending on the extent of the search, border agents' review of information

[1] This opinion does not address the potentially more difficult questions regarding an attorney's duty to protect confidential information while in, or crossing into, foreign countries. While the principles described in this opinion regarding safeguarding clients' confidential information are broadly applicable, efforts reasonably necessary to protect clients' confidences at foreign borders and in foreign countries will vary depending on the laws and practices of those countries. Lawyers must therefore familiarize themselves with those laws and practices and determine what safeguards to adopt before transporting clients' confidential information abroad.

[2] In this respect, border searches apparently differ from Transportation Security Administration (TSA) searches of electronic devices in connection with domestic air travel. This Opinion only addresses ethical issues in connection with international travel.

[3] *See* June 20, 2017 Due Diligence Questions for Kevin McAleenan, Nominee for Commissioner of U.S. Customs and Border Protection (CBP), *available at*: http://msnbcmedia.msn.com/i/MSNBC/Sections/NEWS/170712-cpb-wyden-letter.pdf. According to this policy statement, CBP agents do not condition U.S. citizens' reentry on the provision of passwords; nor do they currently review information that, although not physically resident on the devices, is accessible on remote servers via electronic devices. According to CPB, inspections may reveal that electronic devices contain contraband (*e.g.*, child pornography), or that information on electronic devices reveals a threat to national security. CBP reserves the right to cooperate with other investigative agencies, which may seek other kinds of information on travelers' electronic devices.

[4] U.S. CUSTOMS AND BORDER PATROL, SNAPSHOT: A SUMMARY OF CBP FACTS AND FIGURES (2017), available at https://www.cbp.gov/sites/default/files/assets/documents/2017-Mar/CBP-Snapshot-UPDATE-03022017-FY16-Data.pdf (citing daily statistic of 1,069,266 average daily arrivals in February 2017; only 326,723 were by air). Based on these figures, only approximately 0.017% of all individuals entering the United States on a given day are subject to an electronic device search, even with the increase in such searches in 2017. There are no available statistics evidencing how many of the 5,000 searched devices belonged to members of the bar.

stored on, or accessible via, individuals' electronic devices may lead to the disclosure of substantial information, and therefore constitute a significant intrusion for the selected individuals.[5] Under these circumstances, attorneys would benefit from guidance regarding their ethical obligations prior to crossing a U.S. border and when confronted with a border agent's request to search electronic devices containing clients' confidential information.[6]

This Opinion addresses an attorney's ethical obligations under the Rules with respect to U.S. border searches of electronic devices containing clients' confidential information at three points in time: before the attorney approaches the U.S. border; at the border when U.S. border agents seek to review information on the attorney's electronic device; and after U.S. border agents review clients' confidential information.

Before crossing the U.S. border, both Rule 1.6(c), which requires "reasonable efforts to prevent . . . unauthorized access to" clients' confidential information, and the duty of competence under Rule 1.1, require an attorney to take reasonable measures in advance to avoid disclosing confidential information in the event border agents seek to search the attorney's electronic device. The "reasonableness" standard does not imply that particular protective measures must invariably be adopted in all circumstances to safeguard clients' confidential information; however, this Opinion identifies measures that may satisfy the obligation to safeguard clients' confidences in this situation.

At the border, if government agents seek to search the attorney's electronic device pursuant to a claim of lawful authority,[7] and the device contains clients' confidential information, the attorney may not comply unless "reasonably necessary" under Rule 1.6(b)(6), which permits disclosure of clients' confidential information to comply with "law or court order." Under the Rule, the

[5] *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014) (describing range and extent of information stored on, and accessible via, individuals' cell phones).

[6] These circumstances have prompted the ABA to seek changes and clarifications to existing regulations and practices regarding the treatment of confidential and privileged materials during border searches. *See* AMERICAN BAR ASSOCIATION, PRESERVATION OF ATTORNEY-CLIENT PRIVILEGE AND CLIENT CONFIDENTIALITY FOR U.S. LAWYERS AND THEIR CLIENTS DURING BORDER SEARCHES OF ELECTRONIC DEVICES (May 5, 2017), *available at* https://dlbjbjzgnk95t.cloudfront.net/0921000/921316/letter.pdf.

[7] The legality of a border search of an electronic device is apparently unsettled. *See Abidor v. Napolitano*, 10-cv-04059 (E.D.N.Y. Dec. 31, 2013) (dismissing claims challenging authority of CBP and ICE to detain electronic devices at borders, even absent reasonable suspicion); *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013)(border agents need reasonable suspicion of illegal activity before they could conduct a *forensic* search, aided by sophisticated software, of the defendant's laptop but a *manual* search of a digital device is "routine" and so a warrantless and suspicionless search is "reasonable" under the Fourth Amendment); *United States v. Kim*, 103 F. Supp. 3d 32, 52 (D.D.C. 2015)(suppressing evidence found during a search of a laptop at the border after border agents made an exact copy of the laptop's hard drive and searched it with forensic programs). *See generally* Patrick G. Lee, *Can Customs and Border Official Search Your Phone? These Are Your Rights*, PROPUBLICA (Mar. 13, 2017) https://www.propublica.org/article/can-customs-border-protection-search-phone-legal-rights; U.S. CUSTOMS AND BORDER PATROL DIRECTIVE NO. 3340-049, BORDER SEARCH OF ELECTRONIC DEVICES.CONTAINING INFORMATION (2009) *available at* https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf.

attorney first must take reasonable measures to prevent disclosure of confidential information, which would include informing the border agent that the device or files in question contain privileged or confidential materials, requesting that such materials not be searched or copied, asking to speak to a superior officer and making any other lawful requests to protect the confidential information from disclosure. To demonstrate that the device contains attorney-client materials, the attorney should carry proof of bar membership, such as an attorney ID card, when crossing a U.S. border.

Finally, if the attorney discloses clients' confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures pursuant to Rule 1.4.

II. Before Crossing the U.S. Border Attorneys Must Undertake Reasonable Efforts to Protect Confidential Information

Attorneys have a duty under Rule 1.6 to protect clients' confidential information.[8] Rule 1.6(a) provides that an attorney may not knowingly use or disclose confidential information without the client's informed consent or implied authorization. Few principles are more important to our legal system.

Additionally, an attorney's obligation to safeguard clients' confidential information against unintentional or unauthorized disclosure is implicit in the duty of competence under Rule 1.1. *See* ABA Formal Op. 11-459 (Aug. 4, 2011) (an attorney's duty to "act competently to protect the confidentiality of clients' information . . . is implicit in the obligation of Rule 1.1 to 'provide competent representation to a client'"); *cf.* NYCBA Formal Op. 2015-3 (April 2015) ("In our view, the duty of competence includes a duty to exercise reasonable diligence in identifying and avoiding common Internet-based scams, particularly where those scams can harm other existing clients.").

Further, the obligation to safeguard clients' confidences is now codified in Rule 1.6(c), as amended January 1, 2017, which specifically requires attorneys to "make reasonable efforts to prevent the inadvertent or unauthorized use or disclosure of, or unauthorized access to," confidential information obtained from prospective, current, and former clients. *See* Rule 1.1, cmts. [16] & [17]. The duty to protect client confidences from "unauthorized access" refers to access that is not authorized by the *client*. *Cf.* Rule 1.6, cmts. [5] & [13] (indicating that "authorization" must be given by the client, not the lawyer). Consequently, just as lawyers must take reasonable measures to prevent third parties' unlawful access to client confidences, attorneys must refrain from conduct, including otherwise permissible disclosures, that may result in third parties' *lawful* access to a client's confidential information without the client's consent. *See, e.g.*, NYCBA Formal Op. 2017-2 (Feb. 2017) (an attorney may not report attorney misconduct to the disciplinary authority where doing so might lead the disciplinary authority to require the production of a client's confidential information without the client's consent).

[8] Rule 1.6(a) defines "confidential information" as "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."

Prior opinions have recognized, in particular, that the duty to safeguard clients' confidences includes a responsibility to take reasonable protective measures when engaging in electronic communications with clients and in electronically storing clients' confidential information. *See, e.g.*, ABA Formal Op. 477R (May 11, 2017); ABA Formal Op. 11-459 (Aug. 4, 2011); ABA Formal Op. 99-413 (March 10, 1999); Cal. Ethics Op. 2010-179 (Jan. 1, 2010); NYSBA Ethics Op. 842 (Sept. 10, 2010); NYSBA Ethics Op. 709 (Sept. 16, 1998). To be "reasonable," protective measures need not be foolproof: making reasonable efforts "does not mean that the lawyer guarantees that the information is secure from any unauthorized access." NYSBA Ethics Op. 842, *supra*. Further, the adequacy of an attorney's efforts to protect clients' confidences depends upon a multitude of facts. *See, e.g.*, ABA Formal Op. 477R, *supra* ("Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c) includes nonexclusive factors to guide lawyers in making a 'reasonable efforts' determination."); ABA Formal Op. 11-459, *supra* ("particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters").

Rules 1.1 and 1.6(c) require attorneys to make reasonable efforts prior to crossing the U.S. border to avoid or minimize the risk that government agents will review or seize client confidences that are carried on, or accessible on, electronic devices that attorneys carry across the border. Except in the unlikely event that an attorney has each affected client's consent to disclose confidential information during a border search, such disclosure would be "unauthorized" under Rule 1.6(c) and the attorney would be obligated to make "reasonable efforts" to prevent such disclosure from occurring. In the above hypothetical, the attorney has not obtained informed consent from the clients whose confidential information would be affected, as is required to obtain authorization under Rule 1.6(a)(1). Further, it is hard to imagine a situation where disclosure to a government official during a border search would "advance the best interests of the client" and therefore be "impliedly authorized to advance the best interests of the client" under Rule 1.6(a)(2).

The necessary degree of precaution depends on the circumstances, including the sensitivity of the confidential information that is at risk. See Rule 1.6, cmt. [16] (listing relevant considerations). "Reasonableness" by its nature depends on the multiple facts and circumstances of a given situation and does not lend itself to categorical or bright-line rules. If in doubt, an attorney may, and would be well-advised to, take more cautious measures than what is minimally required by Rule 1.6(c).

Comment [16] to Rule 1.6 provides guidance by identifying the following non-exclusive list of factors relevant to the reasonableness of an attorney's efforts:

1. The sensitivity of the information;
2. The likelihood of disclosure if additional safeguards are not employed;
3. The cost of employing additional safeguards;
4. The difficulty of implementing the safeguards; and
5. The extent to which the safeguards adversely affect the attorney's ability to represent clients (e.g., by making a device or software excessively difficult to use).

Thus, the various facts and circumstances bearing on whether protective efforts are "reasonable" to avoid disclosing client confidences at the border – and therefore minimally required by Rule

1.6(c) – may include the type and nature of the confidential information involved; the need to bring the information across the border in the first instance; the safeguards used by the attorney; the availability, costs, and challenges associated with implementing additional safeguards; an attorney's resources and capabilities; and any factors that may affect the likelihood of disclosure, such as the jurisdiction from which the attorney is returning. Among other things, these considerations suggest that an attorney should not carry clients' confidential information on an electronic device across the border except where there is a professional need to do so, and especially that attorneys should not carry clients' highly sensitive information except where the professional need is compelling.[9]

Given the rapid pace of technological development and the disparities between the practices, capabilities, and resources of attorneys, it would be difficult or impossible to identify a list of minimum mandatory prophylactic or technical measures for an attorney to adopt before crossing the U.S. border. Not only would such a list run the risk of quickly becoming obsolete, but it would also be of limited use, since "reasonableness" standards are not amenable to a one-size-fits-all analysis. Moreover, expectations regarding reasonable efforts are likely to evolve over time as the relevant technology changes, as practices regarding border searches and knowledge of those practices develop, and as attorneys become increasingly aware of the risks of disclosure and the available means to avoid them. However, as discussed below, an attorney must generally (i) evaluate the risks presented by traveling with confidential information and (ii) based on the risk analysis, consider what safeguards to employ to limit or reduce the risk that confidential information will be accessed or disclosed in the event of a search. While no particular safeguard is invariably required by the Rules as long as the attorney's protective efforts are "reasonable," we recommend that attorneys consider adopting the following safeguards to protect confidential information or to reduce the risk of its disclosure.

i. Evaluating the Risk of Disclosure and Potential Harms that May Result

An attorney must evaluate the risks associated with crossing the U.S. border while in possession of clients' confidential information, including the likelihood that border agents will demand and secure disclosure of clients' confidential information, the sensitivity of the information carried, and the harm that would result if the information were disclosed. This requires familiarity with the relevant laws and practices regarding border searches of electronic devices whenever an attorney opts to carry a device that contains, or can access, clients' confidential information. *Cf.* NYSBA Ethics Op. 782 (Dec. 8, 2004) (requiring lawyers to use "reasonable care" to stay abreast of technological advances and the potential risks associated with using, storing, maintaining, accessing, and transmitting confidential information).

Although, as noted above, U.S. border searches of electronic devices (at the time of this opinion's publication) are relatively infrequent, any unauthorized disclosure of a client's

[9] An attorney whose client outside the United States provides electronically-stored confidential information (*e.g.*, on a thumb drive) must "reasonably consult with the client about the means by which the client's objectives are to be accomplished." Rule 1.4(a)(2). The attorney should consider whether this obligation triggers, under all the circumstances, the need for a discussion concerning the manner in which the client's confidential information will be transported and the attendant risks.

confidential information entails a violation of the client's expectation of confidentiality and is presumptively harmful, regardless of whether the unauthorized recipient otherwise uses the information to the client's detriment. *See, e.g.*, NYCBA Formal Op. 2017-2, *supra* (attorney may not provide client's confidential information to the disciplinary authority without the client's consent, even if the client would not be "embarrassed or harmed if the information were disclosed to the disciplinary authority specifically"). Moreover, even if a border search seems highly unlikely, that consideration should be weighed against the amount and sensitivity of the information held and any additional harm that may result from its disclosure without the client's consent. [10] For certain lawyers, practices, organizations, or clients, providing government agencies with access to sensitive confidential data can cause significant harm, which would strongly suggest in such circumstances that it would be unreasonable to carry confidential information that may be disclosed to border agents, even for legitimate professional reasons, if avoidable.

ii. Implementing Safeguards

Attorneys must also evaluate the efficacy, cost, and difficulty associated with implementing safeguards to prevent or limit confidential information. Rule 1.6, cmt. [16].[11] As discussed above, whether safeguards are ultimately required as minimally "reasonable efforts" depends on the circumstances of each such situation.

The simplest option with the lowest risk is not to carry any confidential information across the border. One method of avoiding the electronic transportation of clients' confidences involves using a blank "burner" phone or laptop, or otherwise removing confidential information from one's carried device by deleting confidential files using software designed to securely delete information, turning off syncing of cloud services, signing out of web-based services, and/or uninstalling applications that provide local or remote access to confidential information prior crossing to the border.[12] This is not to say that attorneys traveling with electronic devices must remove all electronically stored information. Some electronic information, including many work-related emails, may contain no confidential information protected by Rule 1.6(a). Even

[10] Traveling attorneys should also be aware that many customs and border protection agencies may demand that the attorney provide access to any information stored on a device (including information that may be otherwise protected or encrypted), and in addition may have access to software tools that allow them to copy the entirety of a device and/or permit the recovery of deleted information that has not been securely deleted using specialized tools. *Test Results for Mobile Device Acquisition*, DEPT. OF HOMELAND SECURITY, https://www.dhs.gov/publication/mobile-device-acquisition (last visited Apr. 11, 2017).

[11] Comment [16] further recognizes that a client may "require the lawyer to implement special security measures not required by this Rule, or . . . give informed consent to forgo security measures that would otherwise be required by this Rule." As this Comment reflects, an attorney may not forgo "reasonable efforts" to protect the client's confidential information, as required by Rule 1.6(c), unless the client gives informed consent. Further, especially when it is necessary to travel with highly sensitive information, an attorney would be well advised to discuss with the client whether to adopt special security measures, beyond those required by Rule 1.6(c) in the situation.

[12] Prior to any such deletion, however, an attorney should ensure that the information deleted is securely backed up so that the attorney may use the information at a later date.

when emails contain confidential information, the obligation to remove these emails from the portable device before crossing the border depends on what is reasonable. As previously discussed, this turns on the ease or inconvenience of avoiding possession of confidential information; the need to maintain access to the particular information and its sensitivity; the risk of a border inspection; and any other relevant considerations.

A lawyer with access to greater resources or who handles more sensitive information should consider technological solutions that permit secure remote access to confidential information without creating local copies on the device; storing confidential information and communications in secure online locations rather than locally on the device; or using encrypted software to attempt to restrict access to mobile devices.

While attorneys thus have various available alternative means of safeguarding clients' confidential information from disclosure at the U.S. border, whatever measures an attorney adopts must, under all the facts and circumstances, be "reasonable" to protect this information.[13]

III. At the U.S. Border Attorneys May Disclose Clients' Confidential Information Only to the Extent "Reasonably Necessary" to Respond to a Government Agent's Claim of Lawful Authority

Assuming an attorney has made reasonable efforts to protect clients' confidential information before crossing the U.S. border, in many cases the attorney will entirely avoid carrying clients' confidential information in an electronic device. In other cases, when attorneys' electronic devices do contain clients' confidential information, the information will be limited to what is professionally necessary, and ideally limited in significance, so that clients would not be significantly harmed by its disclosure. But regardless of how limited or insignificant the information may appear to be, attorneys subject to a border search may disclose clients' confidential information only to the extent permitted by Rule 1.6.

Rule 1.6(a) prohibits attorneys from knowingly disclosing "confidential information" or using such information to the disadvantage of the client, for the lawyer's own advantage, or for the advantage of a third person, unless the client gives informed consent or implied authorization or the disclosure is permitted by Rule 1.6(b). Rule 1.6(b), in turn, permits, but does not require, an attorney to use or disclose confidential information in specified exceptional circumstances, of which only 1.6(b)(6) is relevant to the above-described border-search scenario.

Rule 1.6(b)(6) permits an attorney to "reveal or use" confidential information to the extent the attorney "reasonably believes necessary . . . when permitted or required . . . to comply with other law or court order." Comment [13] to Rule 1.6 recognizes that this exception permits the disclosure of a client's confidential information insofar as reasonably necessary to respond to an order by a "governmental entity claiming authority pursuant to . . . law to compel disclosure." The exception applies even when the validity of the relevant law or court order, or its application, is subject to legal challenge, although, in ordinary circumstances, compliance is not

[13] *See, e.g.,* NYSBA Ethics Op. 1020 (Sept. 12, 2014); NYSBA Ethics Op. 1019 (Aug. 6, 2014); NYSBA Ethics Op. 939 (Oct. 16, 2012); NYSBA Ethics Op. 842 (Sept. 10, 2010); N.Y. State 782 (Dec. 8, 2004).

"reasonably necessary" until any available legal challenge has proven unsuccessful. *See* Rule 1.6, cmt. [13] ("Absent informed consent of the client to comply with the order, the lawyer should assert on behalf of the client nonfrivolous arguments that the order is not authorized by law, the information sought is protected against disclosure by an applicable privilege or other law, or the order is invalid or defective for some other reason.").

In general, disclosure of clients' confidential information is not "reasonably necessary" to comply with law or a court order if there are reasonable, lawful alternatives to disclosure. Even when disclosure is reasonably necessary, the attorney must take reasonably available measures to limit the extent of disclosure. *See, e.g.*, ABA Formal Op. 10-456 (July 14, 2010). For example, compliance with a subpoena or court order to disclose confidential information is not "reasonably necessary" until the attorney or the attorney's client (or former client) has asserted any available non-frivolous claim of attorney-client privilege. *See, e.g.*, NYCBA Formal Op. 2005-3 (March 2005). Likewise, a lawyer must ordinarily test a government agency's request for client confidential information made under color of law. *See, e.g.*, NYCBA Formal Op. 1986-5 (July 1986) ("[I]f presented with a request by a governmental authority for production of information pertaining to escrow accounts when a client is a target of an investigation, a lawyer must, unless the client has consented to disclosure, decline to furnish such information on the ground either that it is protected by the attorney-client privilege or that it has been gained in the course of a confidential relationship. . . . If disclosure is [subsequently] compelled [by a court], it will not breach a lawyer's ethical obligation with respect to his client's confidences or secrets.").

At the same time, attorneys need not assume unreasonable burdens or suffer significant harms in seeking to test a law or court order. *See, e.g.*, NYSBA Ethics Op. 945 (Nov. 7, 2012) (indicating that "when the law governing potential disclosure is unclear, a lawyer need not risk violating a legal or ethical obligation, but may disclose client confidences to the extent the lawyer reasonably believes it is necessary to do so to comply with the relevant law, even if the legal obligation is not free from doubt"). For example, although an attorney must consult with the client about an adverse ruling, *see* Rule 1.4, the attorney need not finance an appeal of the court's ruling much less intentionally defy the trial court and accept a contempt-of-court order. *See, e.g.*, ABA Formal Op. 473 (Feb. 17, 2016) ("Requiring a lawyer to take an appeal when the client is unavailable places significant and undue burdens on the lawyer."); NYCBA Formal Op. 2005-3, *supra* ("Should the court overrule the objection or assertion of privilege or other protection, the attorney may then testify about the privileged or protected material").

Rule 1.6(b)(6) permits an attorney to comply with a border agent's demand, under a claim of lawful authority, for an electronic device containing confidential information during a border search. While legal challenges in court might be made to the relevant law or its application, it would be an unreasonable burden to require that attorneys, having made reasonable efforts to protect clients' confidential information, forgo reentry into the United States or allow themselves to be taken into custody while litigating the lawfulness of a border search. Unless court rulings forbid such border searches, an attorney may ultimately comply with a border agent's demand. Likewise, in this unusual circumstance, it would ordinarily be impracticable and of no utility for attorneys stopped at the border to consult with the affected clients before complying. (The obligation to consult thereafter is addressed below in Part IV.)

That said, compliance is not "reasonably necessary" unless and until an attorney undertakes reasonable efforts to dissuade border agents from reviewing clients' confidential information or to persuade them to limit the extent of their review. *Accord* Rule 1.6(c) (requiring "reasonable efforts" to protect clients' confidential information). Such efforts would include informing the border agent that the subject devices or files contain privileged or confidential materials, requesting that such materials not be searched or copied, asking to speak to a superior officer and making any other reasonably available efforts to protect the confidential information from disclosure. To add credence to the claim of attorney-client privilege, an attorney should carry and be prepared to present some form of attorney identification, such as a court-issued identification or in the very least a business card, when crossing a U.S. border. An attorney should know the relevant law and practices and should consider bringing a printed copy of a given customs agency's policies or guidelines regarding searches of privileged information.[14]

The practical significance of clearly informing the border agent of the presence of confidential or privileged information arises from the regulations of the CBP and the U.S. Immigration and Customs Enforcement Bureau ("ICE"), which each recognize the sensitivity of legal materials. The regulations require a border agent confronted with a claim of legal privilege to seek an additional review or authorization prior to conducting a search of the information that the attorney claims is confidential or privileged. This obligation to obtain further review applies "only to the extent that the agent Officer suspects that the content of such a material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of" CBP or ICE, respectively.[15] Although it is uncertain how border agents apply this "suspicion"

[14] U.S. Customs and Border Patrol Directive No. 3340-049, Border Search of Electronic Devices Containing Information § 5.2.1 (2009) *available at* https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf; U.S. Customs and Border Protection Policy Regarding Border Search of Information (July 16, 2008), *available at* https://www.cbp.gov/sites/default/files/documents/search_authority_2.pdf.

[15] Section 5.2.1 of CBP Directive No. 3340-49, provides: "Officers may encounter materials that appear to be legal in nature, or an individual may assert that certain information is protected by attorney-client or attorney work product privilege. Legal materials are not necessarily exempt from a border search, but they may be subject to the following special handling procedures: If an Officer suspects that the content of such a material may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of CBP, the Officer must seek advice from the CBP Associate/Assistant Chief Counsel before conducting a search of the material, and this consultation shall be noted in appropriate CBP systems of records. CBP counsel will coordinate with the U.S. Attorney's Office as appropriate." U.S. CUSTOMS AND BORDER PATROL DIRECTIVE NO. 3340-049, BORDER SEARCH OF ELECTRONIC DEVICES CONTAINING INFORMATION (2009) *available at* https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf

Section 8.6(2)(b) of the parallel ICE Directive similarly provides: "Special Agents may encounter information that appears to be legal in nature, or an individual may assert that certain information is protected by the attorney-client or attorney work product privilege. If Special Agents suspect that the content of such a document may constitute evidence of a crime or otherwise pertain to a determination within the jurisdiction of ICE, the ICE Office of the Chief Counsel or the appropriate U.S. Attorney's Office must be contacted before beginning or continuing a search of the document and this consultation shall be noted in appropriate ICE systems."

standard in actual searches, attorneys should take advantage of this possible avenue for preventing the disclosure of clients' confidential information.

IV. If Confidential Information Is Disclosed During a Border Search, An Attorney Must Promptly Inform Affected Clients

If an attorney's electronic device containing clients' confidential information is reviewed or seized at the border, the attorney must notify affected clients of what occurred and of the extent to which their confidential information may have been reviewed or seized.[16] This obligation arises out of the general duty under Rule 1.4 to communicate with the client about the status of a matter and about decisions that the client faces in the representation. *See* Rule 1.4(a)(1)(i) & (a)(3); *see also* Rule 1.6, cmt. [13]; *compare* NYCBA Formal Op. 2015-6 (June 2015) ("Given that lawyers have a duty to preserve client files (at least for some period of time), it follows that an attorney may have a duty to notify the client or former client when such files have been inadvertently destroyed."); NYSBA Ethics Op. 1092 (May 11, 2016) ("a lawyer must report to a client a significant error or omission by the lawyer in his or her rendition of legal services"). Disclosure will provide the client an opportunity to determine whether to file a legal challenge, assuming one is available, or to undertake any other available responses. Whether attorneys have legal obligations in this situation independently of the Rules is a question outside the scope of this opinion.

CONCLUSION:

Before crossing the U.S. border, an attorney must make reasonable efforts to protect against the disclosure of clients' confidential information in response to a demand by border agents. Because "reasonable efforts" depend on the circumstances, no particular safeguards are invariably required. However, attorneys should generally (i) evaluate the risks of traveling with confidential information and (ii) consider what safeguards to implement to avoid or reduce the risk that confidential information will be accessed or disclosed in the event of a search. At the border, if government agents seek to search the attorney's electronic device pursuant to a claim of lawful authority, and the device contains clients' confidential information, the attorney may not comply until first making reasonable efforts to assert the attorney-client privilege and to otherwise avert or limit the disclosure of confidential information, e.g., by asking to speak to a superior officer. To add credence to the claim of attorney-client privilege, an attorney should carry attorney identification and be familiar with the customs agency's policies or guidelines regarding searches of privileged information. Finally, if the attorney discloses clients' confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures.

[16] In the context of responding to disclosures as a result of hacking, legal data security experts recommend, where possible, applying forensic analysis to systems after a breach occurs since the appropriate response must be guided by the scope of the breach. A similar approach may be warranted when an electronic device has been confiscated, i.e. a lawyer should take available steps to learn what was disclosed. *See* Allison Grande, *5 Steps to Take When Your Law Firm Is Hacked*, LAW360 (Jul 22, 2014 3:16 PM EDT), https://www.law360.com/articles/556398/5-steps-to-take-when-your-firm-is-hacked.

NYSBA

We're with you at every step, elevating the practice of law with benefits that help grow your law practice.

Get to know your benefits at www.nysba.org/memberbenefits

NYSBA
NEW YORK STATE BAR ASSOCIATION
One Elk Street, Albany, NY 12207
Phone 518.463.3200/800.582.2452
www.nysba.org
www.nysba.org/NYSBACyber

NEW YORK STATE BAR ASSOCIATION

A CYBERSECURITY GUIDE FOR ATTORNEYS

Learn how to protect your law firm's electronic assets. For more information, visit **www.nysba.org/NYSBACyber**.

NYSBA

Lawyers must keep abreast of the risks associated with managing technology and sensitive information, taking steps to safeguard themselves, their firm and their clients.

> *"[C]yber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data.* ***Lawyers can no longer assume that their document systems are of no interest to cyber-crooks.****"*
>
> Committee on Professional Ethics, Opinion 1019 (August 6, 2014)
> (emphasis added)

NYSBA® Protect yourself, your firm and your clients.
www.nysba.org/NYSBACyber

Protect firm computers and networks

Install security and antivirus software that protects against malware or malicious software on mobile devices and computers used within the firm or accessed from outside the office. Secure electronic communications as appropriate, through passwords or encryption, as well as the transmission of data stored in the cloud, ensuring secure "cloud" storage. Scrub "metadata" from electronic communications. Also, use a firewall program to prevent unauthorized access.

Require strong authentication

Ensure that users accessing your firm's network create strong user IDs and passwords/passcodes for computers, mobile devices and online accounts. Make sure users are accessing official websites when entering passwords/passcodes using a mix of upper and lower case letters, numbers, symbols and/or long, uncommon phrases. Differentiate passwords/passcodes on devices and/or accounts, changing them regularly in order to maintain passwords/passcodes in a secure manner. Be sure to never provide your passwords/passcodes to others.

Provide firm education

Establish security practices and policies for all firm employees. Monitor employees and enforce best practices pertaining to internet usage guidelines for mobile devices, internet usage, email and social media. Do not update software and apps unilaterally; instead, updates should be done after inquiry to the responsible individual or department. Identify an individual/department responsible for the above monitoring and advise all firm employees of the need to update devices upon consultation with appropriate personnel at the firm.

Access information on secure internet connections

Connect to the internet using only secure wireless network connections to ensure a private connection, such as a VPN. Public internet provided at airports, hotels and/or internet cafés may not be secure.

Suspicious emails, attachments and unverified apps/programs

Be suspicious of opening, forwarding or responding to unsolicited emails and attachments or links from unknown sources and be sure to charge phones on reliable USB ports. Do not download apps/programs from unverified sources to your computer or mobile devices, especially apps/programs that have access to contacts or other information on your mobile devices. Log out of apps/programs instead of simply closing the internet browser. And avoid file sharing services.

Software updates

Software vendors regularly provide patches and/or updates to their products to correct security flaws and improve functionality. Ensure timely patches and antivirus software updates are installed in all devices.

The Con of Social Engineering: Law Firms are Easy Prey

A discussion of the threat that social engineering (aka the "human side of hacking") poses to law firms, and some tips and practical guidelines to reduce its effectiveness.

By **Mark A. Berman, Ronald J. Hedges, and Kennet Westby** | June 01, 2018 at 03:00 PM

If the movies formed your understanding of cybersecurity threats against the legal profession, you would believe that criminal syndicates are *hacking* into law firms constantly. These organizations would apparently have endless technology and gadgets, penetrating networks using the most sophisticated "James Bond" techniques that even the best defenses in the world could not possibly thwart. Recent news reports do not paint a much better picture of the many "bad guys" getting access to confidential information and data entrusted to both big and small law firms. The reality is different and much less glamorous and sophisticated than we see in the media.

The truth is, however, that law firms are responsible for safekeeping some of the most valuable, sensitive and highly confidential information of companies and individuals. The breadth and value of that information makes them a lucrative target for so many different types of bad guys that span almost every human threat vector one can model. The other reality is that, while most of these attackers are motivated, very few of them have evil lairs filled with supercomputers and spy gadgets in their arsenal. Unlike the movies, however, they unfortunately do not need those tools to be successful bad guys against law firms.

The Threat

"Social engineering" is the human side of *hacking* that does not involve the cracking of passcodes or infiltration of networks. It uses information a bad guy may have gained by, for instance, utilizing a public search engine to find out about a partner, associate, employee or client or even a case or a corporate or real estate transaction, and convincing an individual to click on a malicious (though seemingly *bona fide*) file directed at them by using accurate information that was easily uncovered from routine Internet searches. Once the file is clicked, all the external "super" defenses the law firm has put in place, such as firewalls, spam filters and dual authentication, have little chance of stopping the theft. Social engineering is targeted at all levels of a firm from the receptionist, paralegals, accounting staff, lawyers, to even the firm's information technology professionals. It is the single most effective and actively used method by the bad guys in targeting law firms. It is also the cheapest and easiest to effectuate, thus allowing even low-level crooks to be successful.

Social engineering is based on manipulating a person, usually by providing enough relevant information in context to make their requested action appear to be trustworthy. This can be as simple as a legitimate request asking for confirmation of a password or as complex as asking an individual to run software to create false "back-up" files for the law firm's disaster recovery testing. Social engineering is such a critical tool in *hacking* a law firm that over 90 percent of successful penetration tests against law firms have social engineering as a foundational element of the attack. Removing or minimizing social engineering from the bad guys' tool box makes successfully attacking a law firm exponentially more expensive and complex, and therefore less likely to succeed.

The great news is that law firms have readily available steps to dramatically reduce the effectiveness of social engineering ploys and they do not require *Mission Impossible* technology. Social engineering is all about exploiting gaps in humans' knowledge and awareness. Law firms investing in cyber social engineering awareness training and regular training of the firm's employees, contractors and even clients will create a powerful first line of defense against this method of attack and remove the bad guys' most effective weapon.

The four top methods of social engineering include phishing (email), vishing (phone), phishing (texting) and impersonation (face-to-face). Each method utilizes unique tactics to create trust and authenticity in the ultimate communication used to defraud the recipient. The more repetition there is of personalized, detailed or highly focused communications, the higher the rate of success there will be in convincing the recipient to let down her defenses and for her to click on, open or run malignant communications. Combining each of these different methods, and a *hacker* may even acknowledge in such communication an individual's security training, can produce great results for the *hacker*.

Training and Testing

Training needs to provide tools to help employees validate the *bona fides* of the sender of the electronic communication regardless of the method of communication used. Also providing varied examples of how social engineering attacks may occur will get employees thinking outside the standard security box. Often, attackers play on an individual's weakness, susceptibility and curiosity. The email impersonating someone from human resources or finance with a simple sentence of "Bill, do you really think these expenses should be approved?" with a malicious file attached to it will get hits almost every time. After monitoring news accounts and press releases and performing other "due diligence" on an unsuspecting employee, such as a company bookkeeper, sending a feigned wire instruction to him just when a transaction is about to close and indicating that payment needs to be made by a certain time for the deal to close often works like a charm to cause payment to be made to the bad guy. Role playing or gaming in employee training will make individuals more aware of their susceptibility to such ruses.

In addition to social engineering training, which is your first line of defense, do not forget to do regular real-world testing. Bring in security professionals, who understand up-to-date social engineering artifices, to challenge your investment in "behavior modification" training of your employees and hopefully validate it and improve your security system. Empowering your law firm's employees with such cyber fighting skills also can be a huge morale boost transforming them from victims to warriors in the battle to protect confidential client and law firm information. Building a training and awareness environment which seeks to keep this knowledge and awareness fresh, relevant, frequent and varied in its means of delivery will make it effective.

Practical Guidelines

Security information, resources and tools are provided by many legal associations and, as set forth below, some very practical guidelines offered by the New York State Bar Association at www.nysba.org/nysbacyber/.

Protect firm computers and networks

Install security and antivirus software that protects against malware or malicious software on mobile device and computers used within the firm or accessed from outside the office. Secure electronic communications as appropriate, through passwords or encryption, as well as the transmission of data stored in the cloud, ensuring secure "cloud" storage. Scrub "metadata" from electronic communications. Also, use a firewall program to prevent unauthorized access.

Require Strong Authentication

Ensure that users accessing your firm's network create strong user IDs and passwords/passcodes for computers, mobile devices and online accounts. Make sure users are accessing official websites when entering passwords/passcodes using a mix of upper and lower case letters, numbers, symbols and/or long, uncommon phrases. Differentiate passwords/passcodes on devices and/or accounts, changing them regularly in order to maintain passwords/passcodes in a secure manner. Be sure to never provide your passwords/passcodes to others.

Provide Firm Education

Establish security practices and policies for all firm employees. Monitor employees and enforce best practices pertaining to Internet usage guidelines for mobile devices, Internet usage, email and social media. Do not update software and apps unilaterally; instead, updates should be done after inquiry to the responsible individual or department. Identify an individual/department responsible for the above monitoring and advise all firm employees of the need to update devices upon consultation with appropriate personnel at the firm.

Access Information on Secure Internet Connections

Connect to the Internet using only secure wireless network connections to ensure a private connection, such as a VPN. Public Internet provided at airports, hotels and/or Internet cafés may not be secure.

Suspicious Emails, Attachments and Unverified Apps/Programs

Be suspicious of opening, forwarding or responding to unsolicited emails and attachments or links from unknown sources and be sure to charge phones on reliable USB ports. Do not download apps/programs from unverified sources to your computer or mobile devices, especially apps/programs that have access to contacts or other information on your mobile devices. Log out of apps/programs instead of simply closing the Internet browser. And avoid file sharing services.

Software Updates

Software vendors regularly provide patches and/or updates to their products to correct security flaws and improve functionality. Ensure timely patches and antivirus software updates are installed in all devices.

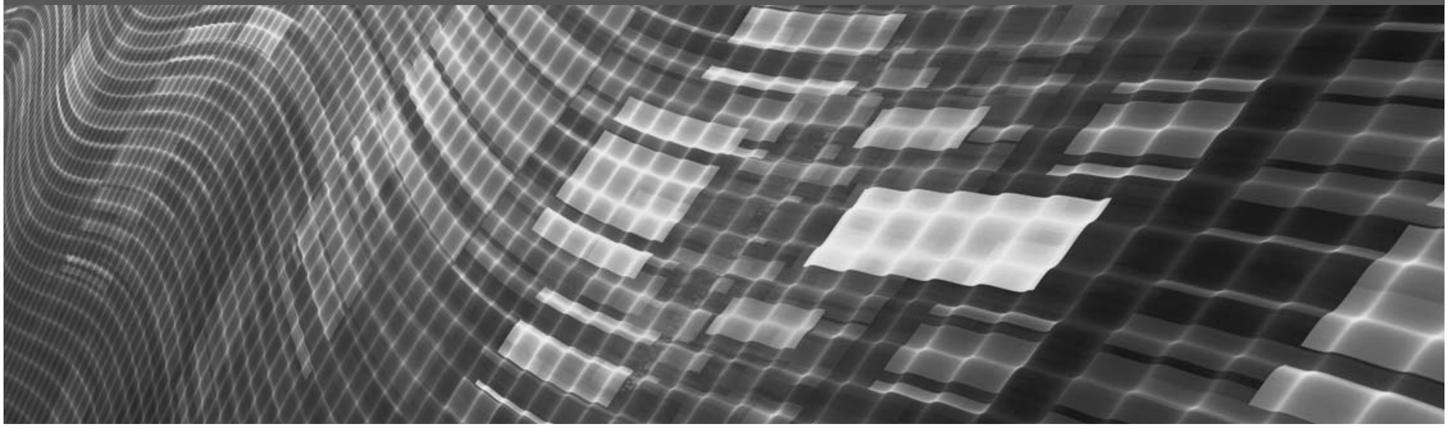
Mark A. Berman, a partner at Ganfer & Shore, chairs the New York State Bar Association's Committee on Technology and the Legal Profession. Ronald J. Hedges, senior counsel at Dentons and a former U.S. Magistrate Judge, is also a member of the Committee. Kennet Westby, Chief Security Strategist at Coalfire, is a member of the Cybersecurity Subcommittee of the Committee.

Topic II

Blockchain and Cybercurrency

BLANKROME

Blockchain Technology & Digital Currencies



SEPTEMBER 2018 • NO. 5

AT&T Sued for $224 Million after Cryptocurrency Theft

Recent lawsuit by cryptocurrency investor seeking $200 million in damages highlights the importance of data protection policies and the potential risk exposure to litigation in the cryptocurrency sector.

On August 15, 2018, in ***Terpin v. AT&T, et al.***, Case No. 18-cv-6975 (C.D. Cal), Michael Terpin, a cryptocurrency investor, filed suit against AT&T, claiming the cell phone provider failed to protect his personal information. Terpin's accounts were recently hacked, causing him to lose nearly $24 million in cryptocurrency. In the lawsuit, Terpin blames AT&T for the hack because it allegedly provided hackers with access to Terpin's telephone number without adhering to its security procedures by enabling SIM swapping, a fraud by which hackers trick a cell phone provider into transferring the target's phone number to a SIM card controlled by the criminal so the criminal can reset the target's passwords and break into accounts. According to Terpin, AT&T knew SIM swapping fraud was widespread—and that its own employees were sometimes involved—and yet has done nothing to protect customers' private information. It was through SIM swapping that hackers were able to drain Terpin's cryptocurrency accounts.

The complaint against AT&T brings 16 counts, including violations of the Federal Communication Act, breach of the AT&T privacy policy, negligence, and unfair competition. Terpin seeks $24 million in compensatory damages and a whopping $200 million in punitive damages.

Businesses that collect and store individual's personal information should be mindful that it is increasingly more important to keep that information secure. As the technological landscape changes and cryptocurrencies gain popularity, data breaches may become even more expensive for businesses if they enable hackers to steal cryptocurrencies. If you have questions about your data protection polices, you should contact an attorney.

For more information, please contact:

Michelle Ann Gitlitz
212.885.5068 | mgitlitz@blankrome.com

Ann E. Querns
215.569.5674 |aquerns@blankrome.com

Notice: The purpose of this update is to identify select developments that may be of interest to readers. The information contained herein is abridged and summarized from various sources, the accuracy and completeness of which cannot be assured. This update should not be construed as legal advice or opinion, and is not a substitute for the advice of counsel.

The Legal Intelligencer

Can the Law Keep Up With the Internet of Things?

In 1999, renowned inventor and self-described futurist Ray Kurzweil—now director of engineering at Google—published "The Age of Spiritual Machines," in which he proposed a formula for calculating the rate of change in evolutionary systems.

By **Jeffrey N. Rosenthal and Thomas F. Brier Jr.** | November 02, 2018

Jeffrey Rosenthal and Thomas Brier of Blank Rome.

In 1999, renowned inventor and self-described futurist Ray Kurzweil—now director of engineering at Google—published “The Age of Spiritual Machines,” in which he proposed a formula for calculating the rate of change in evolutionary systems. Dubbed “The Law of Accelerating Returns,” Kurzweil’s formula holds that technological progress will occur at an exponential rate. Viewed in relation to human history, this means in the 21st century “we won’t experience 100 years of progress”; instead, the growth rate “will be more like 20,000 years of progress.”

Over the past two decades, Kurzweil's model of technological progress has been validated. Today, the world is home to more internet-connected devices (10 billion) than people. Dubbed the "Internet of Things" (IoT), this interconnected network of digital devices has revolutionized how we interact with the world around us. From driverless cars, to personal drones, to smart homes, the degree to which the IoT has affected contemporary society is nothing short of profound.

Only recently, however, have states started to grapple with the myriad security and privacy concerns implicated by the IoT. In September, California became the first state to pass legislation designed to protect the privacy and security of IoT users from the ever-increasing threat of hacking. But the impact (and adequacy) of this legislation, as well as the future of IoT legislation across the country, remains unknown.

Hack the Planet

As defined by the Federal Trade Commission (FTC), the IoT encompasses "devices or sensors—other than computers, smartphones or tablets—that connect, communicate or transmit information with or between each other through the Internet." Common examples include wearable devices (like Fitbit and the Apple Watch); smart-home devices (like Google's Nest Thermostat and the Kohler Verdera Smart Mirror); and vehicle enhancements (like AT&T's Connected Car).

Like personal computers (PCs) and smartphones, IoT devices collect, store and transmit users' personal data. But unlike a PC or smartphone, IoT products tend to be sold without antivirus software, and do not require users to update their login and password information. As a result, the IoT landscape is considered a goldmine for cybercriminals and hackers.

Take, for example, a baby monitor. Today, many parents monitor their children by placing Wi-Fi video monitors in their bedrooms. But as NPR reported earlier this year, these baby monitors often contain several "easy-to-exploit vulnerabilities" that not only allow hackers to peer inside young children's bedrooms, but also "gain access to a home's Wi-Fi network to get information off computers, possibly for financial gain."

Other IoT-connected products are equally susceptible to hacking. Fiat Chrysler was forced to recall 1.4 million cars in 2015 after a team of cybersecurity researchers hacked a Jeep Cherokee's infotainment system, took control of the steering wheel, disabled the breaks and shut down the engine. The health care industry experienced a similar scare a year later, when the FDA confirmed St. Jude Medical was using implantable cardiac devices (e.g., pacemakers) that possessed "vulnerabilities that could allow a hacker to … deplete the battery or administer incorrect pacing or shocks." And the St. Jude case was followed by the widely reported Mirai botnet attack in October 2016, when attackers hijacked IoT devices around the globe by exploiting a vulnerability in webcams and digital recorders, and then used those devices as a botnet to flood the networking company Dyn with malicious traffic. Because of this attack numerous popular websites—including Twitter, Netflix and Reddit—were forced to temporarily shut down.

California Dreamin' [of Better Security]

To combat the ever-increasing threat of IoT hacking, California recently became the first state to mandate the implementation of security features for IoT devices. The law, which goes into effect in January 2020, covers all internet-connected devices made or sold in California. It specifically requires manufacturers to equip devices with "reasonable security" features designed to protect the device from "unauthorized access, destruction, use, modification or disclosure." Compliance can be accomplished by preprogramming the device with a unique password or requiring users to generate a new password before accessing the device for the first time.

The bill has garnered approval from numerous privacy rights organizations and consumer groups, including the Electronic Frontier Foundation and Privacy Rights Clearinghouse. Experts have lauded the bill's user-specific password requirement as an important step in protecting users' privacy, as default passwords—e.g., "admin" or

"1234"—are easily searchable on Google, and consumers often fail to change default passwords after buying an IoT device. By the same token, the law's use of the term "reasonable" offers an important degree of flexibility—allowing it to be broad enough to cover future technological advancements.

But the bill has received criticism as well. According to security researcher Robert Graham, one of the law's major shortcomings is its failure to protect IoT devices from potentially infecting each other. For example, Graham notes that the law could have offered more protection by requiring IoT devices to be sold in a default "isolation" mode, which "prevents infected laptops/desktops (which are much more under threat than IoT) from spreading to IoT."

Implications

Importantly, California's IoT law, which does not contain a private right of action, is enforceable only by California's attorney general or city attorney, a county counsel or a district attorney. Nevertheless, according to numerous commentators the plaintiffs bar is expected "to ramp up its activity in this space in the near future, to seize on the new security requirements if there's a breach or other major security incident that allegedly lacked proper password security."

California's law may spur additional legislation as well. In June 2018, the U.S. House of Representatives' Committee on Energy and Commerce introduced a bill titled the State of Modern Application, Research, and Trends of IoT Act—otherwise known as the SMART IoT Act—that would empower the Secretary of Commerce to conduct a study of IoT devices, determine federal agency jurisdiction over such devices, provide regulations and resources, and report back to the House Committee within one year. This legislation came on the heels of the Internet of Things Cybersecurity Improvement Act, which was introduced in the Senate in August 2017. Although these bills have yet to be passed, California's initiative may spark a renewed interest in further regulating IoT devices on a national scale.

California’s IoT law is sure to have a significant impact on the IoT landscape in the coming decade. As technology continues to progress, and as resultant security concerns emerge, California is posed to play a starring role in regulating the IoT industry. But whether this cast of characters will grow through additional state or federal legislation is unknown. Either way, the IoT show will go on.

Jeffrey N. Rosenthal *is a partner in Blank Rome’s Philadelphia office. He concentrates his complex corporate litigation practice on consumer and privacy class action defense, and regularly publishes and presents on class action trends, attorney ethics and social media law. Contact him at Rosenthal-j@BlankRome.com.*

Thomas F. Brier, Jr. *is an associate in the firm’s Philadelphia office. He concentrates his litigation practice on a variety of criminal and civil litigation matters, and has written extensively on issues pertaining to data privacy and cybersecurity. Contact him at TBrier@BlankRome.com.*

An introduction to virtual currency money transmission regulation

Michelle Ann Gitlitz & Grant E. Buerstetta
Blank Rome LLP

Introduction

The proliferation of virtual currencies, and activities relating to this new asset class, including how businesses are looking to incorporate blockchain payments to quickly and seamlessly effectuate remittances to locations around the world, raises significant compliance issues with respect to money transmission laws and regulations. This treatise chapter examines when businesses in the virtual currency arena may be obligated to comply with both U.S. federal and state money transmission laws and regulations.

On the federal level, the Financial Crimes Enforcement Network ("FinCEN"), a division of the U.S. Department of the Treasury, exercizes regulatory authority pursuant to the Currency and Financial Transactions Reporting Act of 1970, as amended by Title III of the USA PATRIOT Act of 2001 and other legislation, which legislative framework is commonly referred to as the Bank Secrecy Act ("BSA").[1] The BSA is a comprehensive federal anti-money laundering ("AML") and counter-terrorism financing ("CTF") statute. FinCEN is charged with protecting the financial system from being used for money laundering and to prevent terrorism financing. Accordingly, the federal government is primarily concerned with preventing criminals from laundering money or otherwise participating in illegal financial activities. The laws are in place to allow FinCEN to manage the collection, processing, storage, dissemination, and protection of data filed pursuant to its reporting requirements in order to monitor personal information or transactional data.

The data is analysed by FinCEN, which allocates its resources to the areas that pose the greatest financial crime risk. FinCEN also shares information with foreign financial intelligence unit counterparts on AML and CTF efforts. Specifically, FinCEN recently announced that it is sharing its experience on virtual currency with foreign partners through the Egmont Group of Financial Intelligence Units ("FIU") and other international forums. The goal is to help FIUs better advise reporting entities on what to report about virtual currency transactions or activity and other relevant information for revealing important methods and constituents involved in financing illicit activities.

In addition to the federal regime, any entity operating in the virtual currency arena must also consider the intricate (and often confusing) web of state money transmission laws with which they may have to comply. State money transmission regulations are not aimed at protecting against money laundering and terrorist financing; they focus on consumer protection to ensure that a money transmitter will not lose, steal, or misdirect the consumer's money. Virtually every state has its own money transmission licensing regime, which is inefficient, particularly in the context of virtual currency businesses whose technologies and products may operate fluidly across state lines.

The maze of state licensing regulations, paired with FinCEN's federal requirements, demand thoughtful consideration of legal compliance for any person or business who operates in the virtual currency industry and may be considered a money transmitter.

Federal virtual currency money transmission

The BSA requires that "financial institutions," businesses offering a wide array of broadly-defined financial services, surveil their customers and provide information about those customers to FinCEN.[2] Financial institutions must take a number of precautions against financial crime, including establishing Know Your Customer ("KYC") and AML programs and the filing of Suspicious Activity Reports ("SARs") and Currency Transaction Reports ("CTRs") that are used in criminal, tax, and regulatory investigations and proceedings and certain intelligence and counter-terrorism matters.[3]

"Financial institution" includes any bank, broker or dealer in securities, money services business, telegraph company, casino, card club, or a person subject to supervision by any state or federal bank supervisory authority, and that status is determined based on the type of activities in which that person or entity engages.[4] A "money services business," which includes a money transmitter, is the financial institution most relevant to this treatise.

The definition of money transmitter for purposes of BSA regulations includes:

(a) [a]ny person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both, or an electronic funds transfer network; or

(b) [a]ny other person engaged as a business in the transfer of funds.[5]

Whether a person is a money transmitter, including those operating in the virtual currency arena, is a matter of facts and circumstances.[6] The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[7] In 2011, FinCEN issued a final rule amending definitions and other regulations relating to money services businesses to provide that money transmission covers the acceptance and transmission of value that substitutes for currency.[8] Simply put, when a person accepts and transmits anything of value that substitutes for currency, that person is deemed a money transmitter. The regulations specifically exempt from money transmitter status a person who only provides the delivery, communication, or network data access services used by a money transmitter to supply money transmission services; for example, when the only type of brokerage services offered by a person are those in which the buyer makes payment directly to the seller.[9]

FinCEN virtual currency guidance

FinCEN issues guidance on various issues that arise under FinCEN regulations (hereinafter, collectively, the "Guidance"), which is intended to clarify issues or respond to questions of general applicability.[10] FinCEN first addressed rulemaking authority over virtual currency in March 2013, clarifying that it would regulate transmitters of virtual currency in the same manner as transmitters of fiat currency.[11]

Under FinCEN regulations, fiat currency (also referred to as "real" currency) is defined as "the coin and paper money of the United States or of any other country: [i] that is designated as legal tender; [ii] that circulates; and [iii] is customarily used and accepted as a medium of exchange in the country of issuance."[12] "'Virtual' currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency."[13] The Guidance issued in March 2013 addressed "convertible virtual currency," which is defined as either having "an equivalent value in real currency, or acts as a substitute for real currency."[14] FinCEN regulations cover both transactions where the parties are exchanging fiat and convertible virtual currency, as well as transactions from one virtual currency to another virtual currency. Businesses providing anonymizing services (also known as "mixers" or "tumblers"), which attempt to conceal the source of the transmission of virtual currency, are money transmitters when they accept and transmit convertible virtual currency and, therefore, have regulatory obligations under the BSA.[15]

The convertibility of the virtual currency is an important distinction. If a virtual currency cannot be converted to or sold for real currency and does not have any monetary value on the open market, then it does not implicate federal money transmission laws.

The Guidance refers to three categories of participants in the virtual currency ecosystem: users, exchangers, and administrators as explained below.[16]

- **User**: a person who obtains virtual currency to purchase goods or services.[17] In January 2014, this definition was expanded to also include businesses that are strictly investing in convertible virtual currency for their own account and not for any other party.[18] Under the current Guidance, it would appear that institutions investing in virtual currencies such as co-mingled investment funds are considered users.
- **Exchanger**: a person ***engaged as a business*** in the exchange of virtual currency for real currency, funds, or other virtual currency. Note that a person must be engaged in a business; thus, trading simply for personal investment purposes does not qualify one as an exchanger. In addition, one must accept ***and*** transmit virtual currency from one person to another or to another location, such as a brokerage service or trading platform. Mere acceptance of virtual currency in exchange for providing a good or service does not make a person a money transmitter.
- **Administrator**: a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.[19]

Users are not considered money transmitters, and thus are not required to register with FinCEN. Exchangers or administrators may operate as money transmitters and may be required to register with FinCEN depending on the specific facts and circumstances.

Since issuing the Guidance in March 2013, FinCEN has issued other Guidance and rulings on virtual currency that further inform the application of existing money transmission regulations: *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014) (the "2014 Software and

Investment Guidance"); *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001 (Jan. 30, 2014) (the "2014 Mining Guidance"); and *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System*, FIN-2014-R012 (Oct. 27, 2014) (the "2014 Payment System Ruling").

Classification of persons and entities conducting virtual currency business activities for money transmission purposes

The aforementioned Guidance provides insight into how to apply the FinCEN standards of when registration is necessary to various players in the virtual currency market. How FinCEN's Guidance might apply to these persons and entities is set forth below:

- **Software developer**: The production and distribution of virtual currency-related software, in and of itself, are not money transmission services and the entity engaged in the activity is not a money transmitter, even if the purpose of the software is to facilitate the sale of virtual currency.[20]
- **Miners**: Miners play a vital role in allowing many decentralized blockchain-based virtual currency systems to operate properly. Mining is important because virtual currencies or tokens such as Bitcoin are initially acquired through mining; unlike paper money, decentralized virtual currencies do not have a central government to issue the currency. This provides a somewhat controlled way to distribute tokens and creates a real incentive for miners to enter the market. Miners also play another vital role; in the traditional banking system, banks maintain an accurate record of parties and details of each transaction; however, since there is no central regulator for decentralized virtual currencies, the miners assume this role.

  Those who mine virtual currencies, whether by "earning," "harvesting," "creating," or "manufacturing," are all classified as users and not money transmitters. Once the virtual currency is mined, a miner, depending on how he/she uses the convertible virtual currency and for whose benefit, may potentially become a money transmitter.[21] Just because the miner acquired the tokens directly by mining them, rather than purchasing or being given them, his/her status as a user is unaffected. Miners may use their mined tokens or currencies to purchase goods, and until they engage in activities that would qualify them as a transmitter, they remain a user.
- **Centralized virtual currencies**: A convertible virtual currency that has a centralized repository is a centralized virtual currency ("CVC"). The repository of a CVC is a money transmitter to the extent that it allows transfers of value between persons or from one location (i.e., a user's account in New York) to another (i.e., that user's account in California). In addition, if the CVC repository accepts currency or its equivalent from a user and privately credits the user with an appropriate portion of the repository's own convertible virtual currency, and then transmits that internally credited value to third parties at the user's direction, the CVC repository is a money transmitter.[22]
- **Decentralized virtual currencies**: A decentralized virtual currency ("DVC") is a virtual currency that has no central repository and no single person who has the ability to issue or redeem the virtual currency. Persons may obtain the virtual currency through their own computing or mining effort or by purchasing the currency. A person who creates units of a DVC and uses it to purchase real or virtual goods and services is a "user" of the convertible virtual currency and is not subject to regulation as a money transmitter. By contrast, a person who creates units of a DVC, and sells those units to another person for real currency or its equivalent and is engaged in that transfer as

a business, is a money transmitter to the extent that he/she is transferring it from one person or location to another person or location. A person who accepts and transmits real currency to one person in exchange for a DVC, but is arguably engaged in the business of providing goods and services, may have a valid argument that he/she is not a money transmitter. The exact scope of the regulation in this context is currently unclear.[23]

- **Wallets**: are secure virtual currency storage systems used to hold and potentially send or receive virtual currency. Most virtual currencies have official or suggested wallets and the use of a wallet is necessary. The wallet contains a public and private key for each virtual currency address. The private key is a secret number that allows the virtual currency to be spent. The public key is used to ensure the wallet holder is the owner of the wallet address and can receive funds. The public key is mathematically derived from the private key. The status of a wallet as a money transmitter is primarily determined by whether or not the wallet company has custody of the private keys for the virtual currency.
  - **Custodial wallets**: Custodial wallet companies are likely money transmitters. They typically accept virtual currencies for users and transmit them when the currencies need to be moved. The custodial wallet is in full control of the transaction and the user could not facilitate the transaction without the participation and action of the wallet provider. Examples of custodial wallet companies include Bitfinex, Bitthumb and Coinbase.
  - **Non-custodial wallets:** Non-custodial wallet companies are likely *not* money transmitters. These wallets never accept or transmit virtual currencies; they are a software tool. The user facilitates the transaction and neither the wallet nor the keys are ever in the possession of the non-custodial wallet company. This entity can be thought of as merely a developer of software used to aid the customer in facilitating his/her own transactions. Examples of non-custodial wallet companies include Jaxx, BitGo and Mycellium.
- **Custodial exchanges**: are virtual currency exchange platforms on which users are able to buy and sell virtual currencies. What distinguishes this type of exchange as custodial is the fact that the exchange is in control of a user's funds, or in other words, the exchange is the custodian of the private keys for the virtual currencies or tokens. Examples of these types of exchanges include Coinbase, GDAX, Kraken, and Bitfinance. Custodial exchanges are money transmitters because they are both buying and selling, and accepting and transmitting virtual currencies.
- **Non-custodial exchanges**: are virtual currency exchange platforms on which users are able to purchase and sell virtual currencies. What makes the non-custodial exchange different from the custodial exchange is that the exchange never takes possession of the user's virtual currency or private keys. Examples include Shape Shift and Evercoin. Non-custodial exchanges are likely not money transmitters. They are merely a source to help connect potential buyers with potential sellers, similar to a message or classifieds board like Craigslist. Because they are never in possession of the currency or private keys, they are never accepting or transmitting, and they are not buying or selling.
- **Token developers**: are the individuals who create a token platform and the virtual currency. Satoshi Nakamoto, the creator of Bitcoin, was the first to develop and release to the public a peer-to-peer digital currency platform. A token developer who either gives away his/her tokens or allows mining is simply distributing his/her

software and, absent other facts, is not a money transmitter.[24] These token developers never accept and transmit tokens, but rather are simply developing and distributing the software in order to allow other users to operate peer-to-peer. Whether token developers are subject to regulation depends on the business they are engaged in and whether they are a DVC or CVC, as discussed above.

A token developer who sells virtual currency or tokens to users, rather than giving them away or allowing users to mine currency, is more complex. A miner who sells the currency he has mined and a developer who sells currency he has created should be treated the same. At the outset, the Guidance does not address these scenarios and there is not yet any case law in the area. However, in FinCEN's first civil enforcement action against a virtual currency exchanger, Ripple Labs Inc., FinCEN alleged that Ripple Labs' currency, XRP, made the developer an exchanger subject to BSA regulation.[25]

Ripple Labs settled, agreeing to a $700,000 penalty and to take certain remedial measures. This settlement is not precedential because it was a negotiated agreement. However, the allegations seemingly contradict the 2014 Software and Investment Guidance and make the treatment of token developers planning to sell their tokens somewhat unclear.

- **Token issuers:** Although no official guidance has been issued, FinCEN has indicated that those who raise money through an Initial Coin Offering ("ICO") may also have to register as money transmitters. A February 13, 2018 letter from FinCEN to U.S. Senator Ron Wyden of the Senate Committee on Finance (the "FinCEN Letter") states that FinCEN is working with the SEC and CFTC to enforce AML obligations of businesses engaged in ICOs.[26] FinCEN was careful to note that not all ICO issuers must register with FinCEN. Instead, whether an issuer must register depends on the nature of the financial activity involved.[27] The FinCEN Letter further states that a developer that sells convertible virtual currency such as Bitcoin (which has an equivalent value in fiat currency and can be exchanged back and forth for fiat currency), including in the form of an ICO, in exchange for another type of value that substitutes for currency, is a money transmitter and must comply with AML requirements. On August 9, 2018, FinCEN Director Kenneth A. Blanco stated in a speech that "[w]hile ICO arrangements vary and, depending on their structure, may be subject to different authorities, one fact remains absolute: FinCEN, and our partners at the SEC and CFTC, expect businesses involved in ICOs to meet all of their AML/CFT obligations."[28]
- **Payment systems**: Virtual currency payment processing systems typically process payments and assist in executing transactions by accepting cash from the buyer, keeping that cash, and then paying the seller with the approximate market value of a virtual currency, or vice versa. By keeping a large reserve of virtual currency at all times, the payment processer is able to act as his/her own currency exchange to supply equivalent virtual currency for the cash supplied by the buyer.

  According to FinCEN, payment processing systems that accept and convert both real and virtual currencies are money transmitters because they are exchangers and, therefore, must register.[29] "An exchanger will be subject to the same obligations under FinCEN regulations regardless of whether the exchanger acts as a broker (attempting to match two (mostly) simultaneous and offsetting transactions involving the acceptance of one type of currency and the transmission of another) or as a dealer (transacting from its own reserve in either convertible virtual currency or real currency)."[30]

There is, however, a carve-out from registration for payment processors when four conditions are met:

(a) the entity providing the service facilitates the purchase of goods or services, or the payment of bills for goods or services (other than money transmission itself);

(b) the entity operates through clearance and settlement systems that admit only BSA-regulated financial institutions;

(c) the entity provides the service pursuant to a formal agreement; and

(d) the entity's agreement must be at a minimum with the seller or creditor that provided the goods or services and receives the funds.[31]

Meeting this exemption requirement can prove difficult.

- **Bitcoin ATMs:** Generally, a fiat currency automated teller machine ("ATM") is not subject to FinCEN regulation as a money services business or money transmitter.[32] Fiat ATMs simply allow a consumer to access his/her own account and his/her own fiat currency. There is no exchange because most fiat ATMs are unable to transmit funds to third parties or accounts at other financial institutions.[33] Bitcoin ATMs, however, are not merely an intermediary between a consumer and his/her personal bank. Bitcoin ATMs function as either one-way (converting fiat currency to Bitcoin) or two-way (converting fiat currency to Bitcoin and Bitcoin to fiat currency) machines. In both instances, these machines may act as intermediaries between buyers and sellers, more as a broker than as a teller. Therefore, Bitcoin ATM operators generally must register with FinCEN as money transmitters.

Registering as a money services business

Once established, money services businesses have 180 days to register with the United States Secretary of the Treasury.[34] Any company or individual serving as a money services business must file a FinCEN Form 107, along with an estimate of business volume for the coming year, information related to the business' ownership and control, and a list of its authorized agents.[35] FinCEN Form 107 requires money services businesses to identify the states in which they have agents and branches, the type of money services activities they plan to carry out (i.e., money transmitter, currency dealer or exchanger, check casher), the number of agents they have authorized to carry out each activity, and the location (financial institution and account number) of their primary transaction account.[36] If accepted, registration must be renewed every two years. If there is any change in ownership or control, transfer of a 10% voting or equity interest, or more than a 50% increase in authorized agents, then the business must re-register.[37]

Money services businesses must comply with recordkeeping, reporting and transaction monitoring requirements under FinCEN regulations. Examples of these requirements include the filing of reports relating to currency in excess of $10,000 received in a trade or business whenever applicable,[38] general recordkeeping maintenance,[39] and, to the extent any transactions constitute "transmittal of funds" under 31 C.F.R. § 1010.100(ddd), then the money services business must comply with the "Funds Transfer Rule" (31 C.F.R. § 1010.410(e)) and the "Funds Travel Rule" (31 C.F.R. § 1010.410(f)). These requirements apply to both domestic and foreign-located convertible virtual currency money transmitters, even if the foreign-located entity has no physical presence in the United States, as long as it does business in whole or substantial part within the United States.[40] Compliance requirements may vary depending on whether or not the business is a peer-to-peer exchange or a large, high-volume exchanger.[41]

Failure to comply with these requirements, including submission of false or materially incomplete information, can result in fines up to $5,000 per violation, or per day of a continued violation, and imprisonment of up to five years.[42] While registration is relatively easy, once registered, the compliance obligations are burdensome.

No action letters/Requests for rulings to federal or state regulators

If a person or entity is clearly a money transmitter, then federal registration with FinCEN is required, as is potential state licensing as discussed below. However, there may be situations in which it is unclear whether a person or entity must register as a money transmitter. In such a circumstance, it is possible to use "no-action" letters or "requests for rulings" from federal and state regulators. These letters allow a person or entity to explain their business activity to the federal or state regulators to address unclear areas of the law, and to clarify whether particular business activities subject the person or entity to registration or licensing requirements under the federal or state regulatory regimes.

State virtual currency money transmission

State money transmission, unlike federal money transmission, requires licensure, not registration. As a pre-requisite to receiving a licence and/or in connection with maintaining a licence, states generally require some combination of: payment of licensing costs; bonding (or other security device); minimum net worth requirements; disclosure of applicant employment history; submission to investigations or examinations; audited financials and periodic financial reporting to the state; prior money transmission or financial services business experience; disclosure of litigation and bankruptcy proceedings; and fingerprinting and background checks. Even if a person or entity is not a money transmitter under the BSA, they may be a money transmitter in any number of states, or vice versa.

A licence is required in any state where the person or company does business, or solicits citizens, regardless of whether or not he/she has any physical presence in the state. Thus, any entity that is planning a global or nationwide rollout of its virtual currency business must satisfy state licensing requirements regardless of where it is physically located. This is particularly onerous to comply with for virtual currency businesses, because virtual currency is a borderless medium of exchange.

States where money transmission licensing or other requirements are necessary for virtual currency activities

Alabama: requires a licence to transmit virtual currencies.[43]

Alaska: requires that a licensee or applicant who requests approval of a licence to provide transmission of virtual currency enter into a Limited Licence Agreement with the Alaska Department of Commerce, Community and Economic Development, Division of Banking and Securities.[44]

Connecticut: requires the licensing of virtual currency storage and transmission.[45]

Georgia: requires a licence to transmit virtual currencies.[46]

Hawaii: requires a licence and fiat reserves equal to the value of virtual currency held for clients.[47]

Idaho: virtual currency exchangers that accept legal tender (e.g., government backed/issued "fiat" currencies) for later delivery to a third party in association with the purchase of a virtual currency must be licensed as a money transmitter with the Department of Finance.[48] Idaho exempts the sale of virtual currency via Bitcoin ATMs from licensing.[49]

New York: a BitLicense is required by the New York State Department of Financial Services to engage in any "Virtual Currency Business Activity," which is broadly defined under the regulations.[50]

North Carolina: requires virtual currency transmitters to obtain a licence and additional insurance. The law provides several exemptions, including for miners, software companies implementing blockchain services such as smart contract platforms, smart property, multi-signature software and non-custodial and non-hosted wallets.[51]

Oregon: the state recently amended the definition of "money" in its money transmission statute (Or. Rev. Stat. §§ 717 *et seq*.) to include virtual currency. In addition, the state requires virtual currency exchanges to be registered as money transmitters.

Vermont: requires virtual currency transmitters to obtain a money transmission licence.[52]

Virginia: requires virtual currency transmitters to obtain a money transmission licence.[53]

Washington: virtual currency transmitters must obtain a money transmission licence. For companies that store virtual currency on behalf of others, there must be a third party security audit, a money transmitter bond which is calculated on the basis of the transmitter's dollar volume and payment's dollar volume from the previous year, and the company must provide certain disclosures to consumers.[54]

Wisconsin: state law does not currently give the Department of Financial Institutions the authority to regulate virtual currency. Therefore, Wisconsin is unable to license or supervize companies whose business activities are limited to those involving virtual currency. However, should the transmission of virtual currency include the involvement of sovereign currency, it may be subject to licensure in Wisconsin depending on how the transaction is structured. Wisconsin encourages companies to consult with legal counsel to determine whether the business activities they plan to conduct meet those defined in Chapter 217, the "Seller of Checks" law, as requiring licensure.[55]

States that have enacted friendly virtual currency licensing regulations or have taken no position on virtual currency activities

Arizona: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Arizona Department of Financial Institutions pursuant to Ariz. Rev. Stat. § 6-1201 *et seq.*

Arkansas: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Arkansas Securities Division pursuant to the Arkansas Uniform Money Services Act, Ark. Code Ann. §§ 23-55-101 *et seq*.[56]

California: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise, but proposes licensing all "digital currency businesses."[57]

Colorado: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Colorado Division of Banking pursuant to the Colorado Money Transmitters Act, Colo. Rev. Stat. §§ 11-110-106 *et seq*.

Delaware: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Delaware Office of the State Bank Commissioner pursuant to 5 Del. Code §§ 2301 *et seq*.

District of Columbia: the district has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the District of Columbia Department of Insurance, Securities, and Banking Bureau pursuant to D.C. Law §§ 26-1001 *et seq*.

Florida: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise, but prohibits the laundering of virtual currency.[58] Some virtual currency businesses have obtained a traditional money transmitter licence from the Florida Office of Financial Regulation pursuant to Fla. Stat. §§ 560.101 *et seq*.

Indiana: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise.

Illinois: the state has no virtual currency money transmission-specific regulations. The Illinois Department of Financial and Professional Regulation has issued Digital Currency Regulatory Guidance stating that virtual currencies are not "money" under the Transmitters of Money Act and exempting the exchange of "digital currencies" from "money transmission" licensing requirements. Some virtual currency businesses have obtained a money transfer licence from the Illinois Department of Financial and Professional Regulation pursuant to 205 Ill. Comp. Stat. 657.

Iowa: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a money services licence from the State of Iowa Division of Banking pursuant to Iowa Code §§ 533C.201 *et seq*.

Kansas: The Kansas Office of the State Bank Commissioner issued guidance regarding the applicability of the Kansas Money Transmitter Act to people or businesses using or transmitting virtual currency.[59] Virtual currency is not considered "money" for the purposes of the Kansas Money Transmitter Act and a person or business engaged solely in transmitting virtual currency is exempt from licensing.[60] Some virtual currency businesses have obtained a traditional money transmitter licence from the Kansas Office of the State Bank Commissioner pursuant to Kan. Stat. Ann. §§ 9-508 *et seq*.

Kentucky: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Kentucky Office of Financial Institutions pursuant to KY. Rev. Stat. §§ 286.11.0001 *et seq*.

Louisiana: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Commissioner of Financial Institutions pursuant to La. Rev. Stat §§ 6:1031 *et seq*.

Maine: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Maine Department of Professional and Financial Regulation, Bureau of Consumer Credit Protection pursuant to Title 32 Me. Rev. Stat. §§ 6101 *et seq*.

Maryland: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise, but the Maryland Department of Labor, Licensing and Regulation has advized consumers that under the federal paradigm, an "administrator" or "exchanger" must register with FinCEN.[2] Some virtual currency businesses have obtained a traditional money transmitter licence from the Maryland Department of Labor, Licensing and Regulation pursuant to Md. Code Ann., Fin. Inst. §§ 12-401 *et seq*.

Massachusetts: the state exempts Bitcoin ATMs from "financial institution" and bitcoins from foreign currency transmission regulations.[61] Businesses involved in the dissemination of virtual currencies on the internet are "market place facilitators" subject to sales or use tax collection.[62] Some virtual currency businesses have obtained a traditional money services business licence from the Massachusetts Office of Consumer Affairs and Business Regulation, Division of Banks, pursuant to 209 CMR 45 *et seq*.

Michigan: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmission licence from the Michigan Department of Licensing and Regulatory Affairs Office of Financial and Insurance Regulation pursuant to the Money Transmissions Services Act, Mich. Comp. Laws §§ 487.1001 *et seq*. Virtual currency transactions are exempt from sales tax and retailers are required to instantly convert the value of the virtual currency to USD as of the day and the exact time of the transaction.[63]

Minnesota: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmission licence from the Department of Commerce Division of Financial Examinations pursuant to Minn. Stat. §§ 53B.01 *et seq*.

Mississippi: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Mississippi Department of Banking and Consumer Finance pursuant to Miss. Code Ann. §§ 75-15-1 *et seq*.

Missouri: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise except that it exempts Bitcoin ATM transactions from sales tax.[64] Some virtual currency businesses have obtained a traditional money transmitter licence from the State of Missouri, Division of Finance pursuant to Mo. Rev. Stat. §§ 361.700 *et seq*.

Montana: the state is notable as being one of the only states not to have enacted a money transmission statute.

Nebraska: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. In an administrative release, the Nebraska Department of Revenue found that the term "currency" does not include Bitcoin or other virtual currency. Proposed legislation, L.B. 691, which was introduced in the legislature in January 2018, would amend the state's money-laundering statutes to account for virtual currencies. Proposed legislation LB 987 establishes regulations focused on businesses engaging in "virtual currency business activity," and creates a tiered system of registration and licensure for companies that want to do business using virtual currencies. Some virtual currency businesses have obtained a traditional money transmitter licence from the Nebraska Department of Banking and Finance pursuant to the Nebraska Money Transmitters Act, Neb. Rev. Stat. §§ 8-2701 *et seq*.

Nevada: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Nevada Department of Business and Industry, Financial Institutions Division, pursuant to Nev. Rev. Stat. Ann. §§ 671.010 *et seq*.

New Hampshire: the state amended its Money Transmitter statute (N.H. Rev. St. Ann. § 399-G:3) to exempt "persons who engage in the business of selling or issuing payment instruments or stored value solely in the form of convertible virtual currency or receive convertible virtual currency for transactions to another location" from the state's money transmission regulation.[65] Some virtual currency businesses have obtained a traditional money transmitter licence from the New Hampshire Banking Department.

New Jersey: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the New Jersey Department of Banking and Insurance pursuant to N.J.S.A 17:15C-1 *et seq.*

New Mexico: the state enacted its Uniform Money Services Act (§§ 58-32-301 (A)(1) *et seq*.) effective January 1, 2017, but the application to virtual currencies is currently unknown. The definition of "money" does not include virtual currencies.

North Dakota: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the North Dakota Department of Financial Institutions pursuant to N.D. Cent. Code §§ 13-09-01 *et seq.*

Ohio: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Ohio Division of Financial Institutions pursuant to Ohio Rev. Code §§ 1315.01 *et seq*.

Oklahoma: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise, but subordinates the rights of merchants accepting Bitcoin to the rights of any security interest in the Bitcoin (traditional money transfers are free and clear of any security interest).[66] Some virtual currency businesses have obtained a traditional money transmitter licence from the Oklahoma Office of the State Bank Commissioner pursuant to 6 Okla. Stat. §§ 1511 *et seq*.

Pennsylvania: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise, but in late 2016, Pennsylvania amended the definition of "money" in its money transmission law to encompass virtual currencies. Some virtual currency businesses have obtained a traditional money transmitter licence from the Pennsylvania Department of Banking and Securities pursuant to 7 P.S. §§ 6101 *et seq*.

Rhode Island: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Rhode Island Department of Business Regulation pursuant to R.I. Gen. Laws §§ 19-14 and 19-14.3.

South Carolina: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise, but the South Carolina Attorney General has published frequently asked questions that disclose that further guidance with respect to the transmission of virtual currencies will be provided in the "near future."[67]

South Dakota: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the South Dakota Department of Labor Regulation, Division of Banking pursuant to S.D. Codified Laws §§ 51A-17-1 and S.D. Admin. R. 20:07:21:01 *et seq*.

Tennessee: the state has issued guidance clarifying that it does not consider virtual currency to be money under its Money Transmitter Act and therefore, no licence is required.[68] Some virtual currency businesses have obtained a traditional money transmitter licence from the Tennessee Department of Financial Institutions pursuant to Tenn. Code. Ann. §§ 45-7-201 *et seq*.

Texas: in Supervisory Memorandum 1037 issued by the Texas Department of Banking, Texas exempted the exchange of virtual currencies from money transmission licensing requirements because it does not consider virtual currency to be money.[69] Some virtual currency businesses have obtained a traditional money transmitter licence from the Texas Department of Banking pursuant to Tex. Fin. Code § 151.001 and Tex. Fin. Code § 151.301.

Utah: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise. Some virtual currency businesses have obtained a traditional money transmitter licence from the Utah Department of Financial Institutions pursuant to Utah Code Ann. §§ 7-25-101 *et seq*.

West Virginia: the state has taken no position on virtual currency money transmission as of the date of publication of this treatise, but prohibits the laundering of cryptocurrencies.[70] Some virtual currency businesses have obtained a traditional money transmitter licence from the West Virginia Division of Financial Institutions pursuant to W. Va. Code §§ 32A-2-1 *et seq*.

Wyoming: the state amended its Money Transmitter Act to exempt virtual currencies from the Wyoming money transmitter licence and regulations.

Attempts to standardize licensing practices

In an attempt to simplify the process and to create some uniformity and efficiency, seven states – Georgia, Illinois, Kansas, Massachusetts, Tennessee, Texas and Washington – have come together to reach a level of reciprocity. In early 2018, these states agreed that if one party state reviews key requirements of state licensing for a money transmitter applicant, including cybersecurity, background checks, and compliance with the BSA, then the other participating states will accept those findings in their own licensing process. This is the first real step toward an integrated 50-state system of licensure and supervision.[71]

Acknowledgments

The authors acknowledge with thanks the contributions to this chapter by Dennis M.P. Ehling, Gregory Cronin and Justin Porter.

* * *

Endnotes

1. 31 U.S.C. §§ 5311-5332.
2. *Id.* § 5321(a)(2).
3. *See* FinCEN, *BSA Requirements for MSBs*, https://www.fincen.gov/bsa-requirements-msbs.
4. 31 C.F.R. § 1010.100(t).
5. *Id.* § 1010.100(ff)(5).
6. *Id.* § 1010.100(ff)(5)(ii).
7. *Id.* § 1010.100(ff)(5)(i)(A).
8. Bank Secrecy Act Regulations – Definitions and other Regulations Relating to Money Services Businesses, 76 FR 43585 (July 21, 2011).
9. 31 C.F.R. § 1010.100(ff)(5)(ii)(A); *see also Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals*, FIN-2015-R001 (August 14, 2015).
10. 31 C.F.R. Chapter X (formerly 31 CFR Part 103).

11. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (Mar. 18, 2013) ("March 2013 Guidance").
12. *Id.* pg. 1.
13. *Id.*
14. *Id.*
15. *See* https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block?utm_source=7-28-18+Member+List&utm_campaign=7b8d25b1ba-EMAIL_CAMPAIGN_2018_01_19_COPY_01&utm_medium=email&utm_term=0_e50a6ec6df-7b8d25b1ba-344964271#_ftn1 (last visited on August 11, 2018).
16. *Id.*
17. *Id.* pg. 2.
18. *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014).
19. FIN-2013-G001 pg. 2.
20. 2014 Software and Investment Guidance pg. 2.
21. 2014 Mining Guidance.
22. FIN-2013-G001 pg. 4.
23. FIN-2013-G001 pg. 5.
24. *See* 2014 Software and Investment Guidance.
25. *See* FinCEN, *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger: Company Agrees to $700,000 Penalty and Remedial Actions*, (May 5, 2015), https://www.fincen.gov/sites/default/files/2016-08/20150505.pdf.
26. The FinCEN Letter is not technically Guidance that must be followed, but the underlying regulations in the FinCEN Letter must be followed.
27. The FinCEN Letter appears to suggest that, at least in certain cases, virtual currency exchanges are subject to the BSA not because they are money services businesses, but because they are broker-dealers.
28. *See* https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block?utm_source=7-28-18+Member+List&utm_campaign=7b8d25b1ba-EMAIL_CAMPAIGN_2018_01_19_COPY_01&utm_medium=email&utm_term=0_e50a6ec6df-7b8d25b1ba-344964271#_ftn1 (last visited on August 11, 2018).
29. 2014 Payment System Ruling.
30. *Id.*
31. 2014 Payment System Ruling pg. 3.
32. *Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services*, FIN-2007-G006 (Dec. 3, 2007).
33. *Id.*
34. 31 U.S.C. § 5330.
35. 31 C.F.R. § 1022.380.
36. *See* FinCEN Form 107 (Mar. 2011).
37. 31 C.F.R. § 1022.380(b)(4).
38. *Id.* § 1027.330.
39. *Id.* § 1027.410.
40. FinCEN pursued enforcement action against BTC-e, an internet-based virtual currency exchange and a foreign located money services business, for failing to implement basic

AML controls that enabled criminals to launder proceeds. FinCEN fined BTC-e $110 million and its administrator, Alexander Vinnik, $12 million – the largest individual penalty ever assessed by FinCEN. FinCEN partnered with the Department of Justice, which pursued BTC-e and Vinnik criminally.

41. *See* FinCEN, *BSA Requirements for MSBs*, https://www.fincen.gov/bsa-requirements-msbs.
42. 18 U.S.C. § 1960.
43. Ala. Code § 8-7A-2(8).
44. *See* https://www.commerce.alaska.gov/web/dbs/LimitedLicenseAgreementOrders.aspx (last visited on August 11, 2018). Some virtual currency businesses such as Coinbase and CoinX have also obtained a traditional money transmitter licence from the Alaska Division of Banking and Securities pursuant to AS 06.55.102, which is limited to the transmission of fiat currency. Alaska's legislature has proposed a bill to define virtual currency and broaden the definition of money transmission to include it. H.B. 180, 30th Legislature, First Session (introduced Mar. 14, 2017).
45. Conn. Gen. Stat. § 36a-598. In February 2018, a bill was proposed (H.B. 5001, 2018 Leg., 2018 Feb. Reg. Sess. Gen. Ass. (Conn. 2018)), which would impose fees to trade or transfer virtual currency. Some virtual currency businesses have obtained a traditional money transmitter licence from the Connecticut Department of Banking.
46. Ga. Code § 7-1-680(26); Ga. Code § 7-1-690(b)(1) (authorizes virtual currency transmission regulations to encourage economic development).
47. HI Rev Stat § 489D-1 (2013); *see* Hawaii Division of Financial Institutions Application available at https://cca.hawaii.gov/dfi/files/2018/04/HI-Money-Transmitter-License-Company-New-App-Checklist.pdf (last visited August 12, 2018). Coinbase exited Hawaii in 2017, requiring Hawaiian customers to close their accounts, stating that it would be impossible for Coinbase to operate in the state given the reserve requirement. In early 2017, the Hawaiian Senate introduced Senate Bill 949, which seeks to clarify that decentralized virtual currency activities are *not* subject to the state's Money Transmitters Act, and establishes a Decentralized Virtual Currency Working Group within the state's Department of Commerce and Consumer Affairs to study whether virtual currencies should be regulated under the Act. Two bills, Senate Bill 2853 and Senate Bill 3082, introduced in the Hawaiian Senate in January 2018, aim to define and include virtual currencies under Hawaii's Money Transmitters Act. The bills would mandate that those transmitting virtual currencies in the state obtain a licence to do so, and that these persons or businesses issue a warning to consumers before enabling such transactions.
48. *See* Idaho Department of Finance, Letter Re: Money Transmissions (Dated July 26, 2016), *available at* https://www.finance.idaho.gov/MoneyTransmitter/Documents/NAOP/Digital%20Currency/2016-07-26.pdf (last visited August 11, 2018) ("An exchanger that sells its own inventory of virtual currency is generally not considered a virtual currency transmitter under the Idaho Money Transmitters Act." However, "an exchanger that holds customer funds while arranging a satisfactory buy/sell order with a third party, and transmits virtual currency… between buyer and seller, will typically be considered a virtual currency transmitter.")
49. Idaho Dep't of Finance, No Action Letter (Oct. 10, 2014).
50. 23 NYCRR 200. The New York State regulatory scheme has been the subject of much criticism and has resulted in an exodus of businesses from New York because of the costs and regulatory requirements associated with the BitLicense. As of the date of this treatise, only eight companies have been granted a BitLicense. Assembly Bill

A9899A to amend certain provisions of the BitLicense is pending in the New York State Legislature.

51. N.C. Gen. Stat. § 53-208.41, *et. seq.*
52. 8 Vt. Stat. Ann. §§ 2500, *et seq*.
53. Va. Code § 6.2-1900.
54. Wash. Rev. Code §§ 19.230.010, *et seq*.
55. *See* https://www.wdfi.org/fi/lfs/soc/ (last visited August 11, 2018). Some virtual currency businesses have obtained a money transmitter licence from Wisconsin.
56. Ark. Code Ann §§ 23-55-101 *et seq*.
57. Assembly Bill 1123 has been introduced for the second time into the California assembly, which proposes to enact the Virtual Currency Act to prohibit a person from engaging in any virtual currency business, unless licensed by the Commissioner or Business Oversight, or is exempt from licensure.
58. Fla. Stat. § 896.101.
59. *See* Kansas Office of the State Bank Commissioner, Guidance Document MT 2014-01, Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act, (June 6, 2014), available at http://www.osbckansas.org/ mt/guidance/mt2014_01_virtual_currency.pdf.
60. *See* Kansas Office of the State Bank Commissioner, Guidance Document MT 2014-01, Regulatory Treatment of Virtual Currencies Under the Kansas Money Transmitter Act, (June 6, 2014), available at http://www.osbckansas.org/mt/guidance/mt2014_01_virtual_currency.pdf (last visited August 11, 2018).
61. *See* Office of the Commissioner of Financial Regulation, Virtual Currencies: Risks for Buying, Selling, Transacting, and Investing - Advisory Notice 14-01, (April 24, 2014), *available at* http://www.dllr.state.md.us/finance/advisories/advisoryvirtual.shtml (last visited August 11, 2018).
62. Mass. Division of Banks, Opinion 14-004 (May 12, 2014).
63. 830 CMRH 1.7(b)(1).
64. *See* Tax Policy Division of the Michigan Dept. of Treasury, Treasury Update, Vol. 1, Issue 1 (November 2015), *available at* https://www.michigan.gov/documents/treasury/Tax-Policy-November2015-Newsletter_504036_7.pdf (last visited August 11, 2018)
65. Missouri Dep't of Revenue, LR 7411, Collection of Sales Tax on Bitcoin Transfers Through an Automated Teller Machine (ATM), (September 12, 2014).
66. *See* H.B. 436, 2017 Leg., 165th Sess. (N.H. 2017).
67. Okla. Stat. § 1-9-332.
68. *See* http://www.scag.gov/money-services-frequently-asked-questions (last visited August 11, 2018).
69. Memo, Tenn. Dep't of Fin. Inst., Regulatory Treatment of Virtual Currencies under the Tennessee Money Transmitter Act (Dec. 16, 2015) *available at* https://www.tn.gov/content/dam/tn/financialinstitutions/new-docs/TDFI%20Memo%20on%20Virtual%20Currency.pdf (last visited August 11, 2018).
70. *See* https://www.dob.texas.gov/public/uploads/files/consumer-information/sm1037.pdf (last visited August 11, 2018).
71. W. Va. Code §§ 61-15-1 *et seq*. *See* Conference of State Bank Supervisors, "State Regulators Take First Step to Standardize Licensing Practices for Fintech Payments", Feb. 6, 2018, https://www.csbs.org/state-regulators-take-first-step-standardize-licensing-practices-fintech-payments.

Michelle Gitlitz
Tel: +1 212 885 5068 / Email: mgitlitz@BlankRome.com

Michelle Gitlitz is a securities lawyer who represents corporations, individuals, investment companies and funds in corporate, regulatory, and litigation matters. She co-leads Blank Rome's Blockchain Technology & Digital Currencies group and regularly advises companies as they bring blockchain technology applications to market, raise capital through coin/token issuances and digital securities offerings, establish digital currency mining operations, form private investment funds and hedge funds that invest in emerging technologies and digital currencies, and navigate through state and federal money transmission rules and regulations.

Michelle is a frequent presenter on the legal and regulatory aspects of blockchain technology and tokenization. She has participated in MIT's Legal Forum for Artificial Intelligence and Blockchain and has lectured on blockchain and tokenization at MIT's Computational Law Course. Michelle also participated in the United Nations' Blockchain for Impact Global Summit. She is a member of the Wall Street Blockchain Alliance, Chamber of Digital Commerce, Global Legal Blockchain Consortium, and the Accord Project. She is also Vice Chair of Blank Rome's Women's Forum and is the co-founder of a non-profit, Diversity in Blockchain, Inc.

Grant Buerstetta
Tel: +1 212 885 5454 / Email: GBuerstetta@BlankRome.com

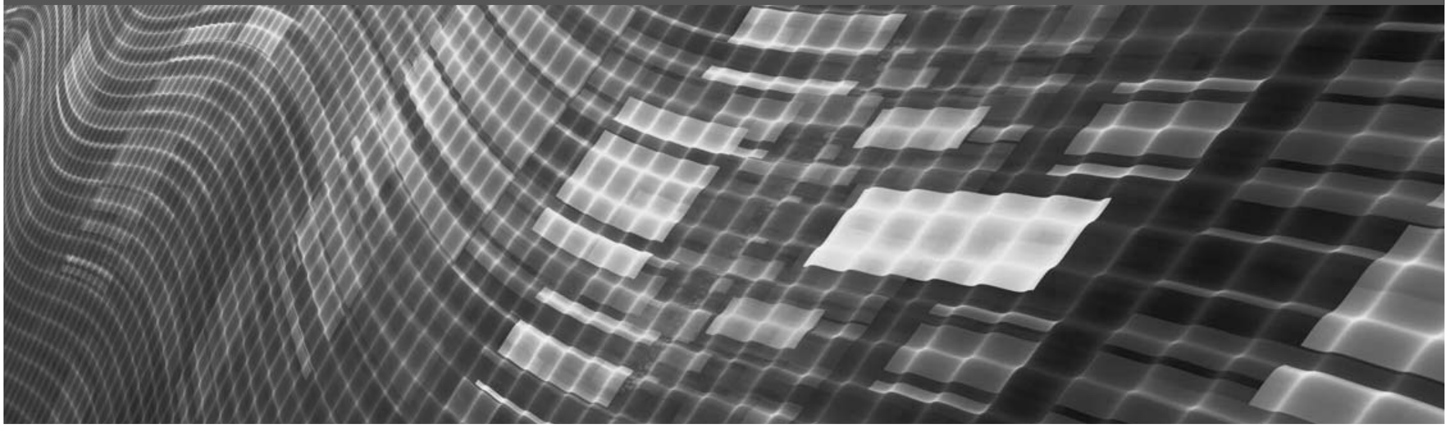
Grant Buerstetta represents financial institutions, asset managers, issuers, and investment funds focused on debt and structured securities and serves clients in areas such as: complex structured and asset-backed securities and securitization transactions; alternative investment fund formation and operation; securities issuances in domestic and international capital markets; and blockchain technology and cryptocurrencies. Grant is the Chair of Blank Rome's Finance, Restructuring and Bankruptcy Practice Group and co-leads Blank Rome's Blockchain Technology & Digital Currencies group. Grant has formed and advises numerous alternative investment funds investing in cryptocurrencies and blockchain infrastructure. Grant's experience with and knowledge of various structured credit products and securities law exemptions benefit his clients in structuring and executing transactions. In addition, Grant advises on legal, regulatory and risk management issues surrounding digital securities offerings. Grant also assists in advising clients on money transmission, securities and related regulatory issues. These representations draw on his broader corporate and securities skills as well as in-depth knowledge of complex transaction structuring.

Blank Rome LLP

The Chrysler Building, 405 Lexington Avenue, New York, NY 10174-0208, USA
Tel: +1 212 885 5000 / Fax: +1 212 885 5001 / URL: www.blankrome.com

BLANKROME

Blockchain Technology & Digital Currencies



NOVEMBER 2018 • NO. 6

On the Road to Reconciling GDPR and Blockchain

European Parliament's Blockchain Resolution lays the framework to reconciling the GDPR and blockchain.

On October 3, 2018, the European Parliament passed a resolution on distributed ledger technologies and blockchain (the "Blockchain Resolution"). The Blockchain Resolution emphasizes the importance of taking an "innovation-friendly" regulatory approach, while also recognizing that it is of the "utmost importance" that blockchain technologies are compliant with the General Data Protection Regulation ("GDPR"). The GDPR is the European Union's ("EU") robust data protection legislation that applies not only to entities established in the EU that process personal data, but also to entities that are established outside of the EU that offer their products or services to EU residents or track the behavior of EU residents. The GDPR mandates that personal data only be processed if there is a lawful basis to do so, and gives rights to data subjects that provide them with significant control over the processing of their personal data. Further regulatory guidance on how the GDPR will be applied to blockchain is needed for blockchain innovation to continue.

The Blockchain Resolution reiterated that blockchain technology promotes the pseudonymization of users but not their anonymization. Anonymization irreversibly destroys any way of connecting the data to a natural person. Pseudonymization de-identifies the data in such a way that, with additional information, connecting the data to a natural person is possible. Although direct identification of individual users of a blockchain network is not possible, indirect identification is possible. Because user data on the blockchain is pseudonymized, it is subject to the GDPR. GDPR compliance is not about the technology, but rather how the technology is used to process personal data, and application of the GDPR's principles to blockchain proves highly challenging. Immutability of data and decentralization of control, arguably the two most innovative aspects of blockchain, inherently conflict with provisions of the GDPR.

One issue that requires further guidance is how to determine which actor is the data controller of a blockchain network. The GDPR was fashioned with the implicit assumption that data in the digital world is controlled by identifiable actors. Blockchain technology seeks to achieve radical decentralization of data by replacing identifiable actors with the public. How does the GDPR apply to blockchain technologies that are not controlled by an identifiable actor? For example, Bitcoin is not controlled.

As far as the GDPR is concerned, it must be possible to identify a data controller. It is the data controller who is ultimately accountable for compliance with the GDPR and liable if the GDPR is breached. Among other obligations, the GDPR requires that data controllers process data lawfully, as defined in the GDPR, or face the consequences.

In a private, permissioned blockchain, determining the data controller is straightforward. The centralized company that runs the blockchain is the data controller for purposes of the GDPR.

Determining who the data controller is for a decentralized, public blockchain becomes difficult, if not impossible. There is currently an intense debate to determine who the data controller should be in these decentralized, public blockchains. There are strong arguments for and against finding that the protocol developer, the actors who host the nodes, the network users, or the publishers of smart contracts should be considered as data controllers. The conclusion of this debate will lead to significant liability for one or several of these actors and will influence future development of public blockchain technologies. Because this uncertainty around data controllership makes it difficult to assess a party's responsibilities and potential liability under the GDPR, further regulatory guidance in this respect is urgently needed.

An additional obstacle arises in the right to erasure and rectification of data. Blockchains are immutable. True blockchain rely on the logging and storing of data chains. Prohibiting data modification or removal enables trust in a decentralized blockchain. Thus, deleting data would disrupt the chain and undermine the rationale behind blockchain. How does one reconcile that with the "right of rectification" and "right of erasure?" One potential solution posed by the EU Blockchain Observatory and Forum's October 16, 2018, report on blockchain and the GDPR would be to use blockchain to store immutable proofs that certain data exists and store the data itself outside of the blockchain.

It is important to note that a Resolution from the European Parliament is not legally binding. A Resolution merely seeks to set forth the parliament's position, with a view to promote other EU institutions to enact legislation accordingly. In the Blockchain Resolution, the European Parliament clearly expressed a position to support blockchain and the need for further regulatory clarity regarding blockchain and the GDPR. It is likely that the Blockchain Resolution will lead to further pro-blockchain policy and legislation.

For more information, please contact:

Michelle Ann Gitlitz
212.885.5068 | mgitlitz@blankrome.com

Jennifer J. Daniels
412.932.2754 | daniels@blankrome.com

Michael C. Lupton
212.885.5437 | mlupton@blankrome.com

Notice: The purpose of this update is to identify select developments that may be of interest to readers. The information contained herein is abridged and summarized from various sources, the accuracy and completeness of which cannot be assured. This update should not be construed as legal advice or opinion, and is not a substitute for the advice of counsel.

Volume 2, No. 1 | January–February 2019

RAIL The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL The Journal of Robotics, Artificial Intelligence & Law

Volume 2, No. 1 | January–February 2019

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2019 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquires and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@
meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please call:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Will "Leaky" Machine Learning Usher in a New Wave of Lawsuits?

Brian Wm. Higgins*

This article examines the causes of action that might be asserted against a developer who publishes, either directly or via a machine learning as a service cloud platform. A leaky machine learning model is also explored along with possible defenses, using the lessons of cybersecurity litigation to frame the discussion.

A computer science professor at Cornell University has a new twist on Marc Andreessen's pronouncement that software is "eating the world."[1] According to Vitaly Shmatikov,[2] it is "machine learning [that] is eating the world" today. His personification is clear: machine learning and other applications of artificial intelligence ("AI") are disrupting society at a rate that shows little sign of leveling off. And with increasing numbers of companies and individual developers producing customer-facing AI systems, it seems all but inevitable that some of those systems will create unintended and unforeseen consequences, including harm to individuals and society at large.

Researchers like Shmatikov and his colleagues are starting to reveal those consequences, including one—"leaky" machine learning models—that could have serious legal implications. Below, the causes of action that might be asserted against a developer who publishes, either directly or via a machine learning as a service ("MLaaS") cloud platform, a leaky machine learning model are explored along with possible defenses, using the lessons of cybersecurity litigation to frame the discussion.

Background

Over the last nearly two decades, both the plaintiffs and defendants bars have contributed to a body of case law now commonly referred to as cybersecurity law. The development of this practice

Robotics, Artificial Intelligence & Law / January–February 2019, Vol. 2, No. 1, pp. 9–16.
© 2019 Full Court Press. All rights reserved.
ISSN 2575-5633 (print) / ISSN 2575-5617 (online)

area was inevitable, given the estimated 8,000 data breaches involving 11 billion data records made public since 2005.[3]

After some well-publicized breaches, lawsuits against companies reporting data thefts began appearing more frequently on court dockets across the country. Law firms responded by marketing "cybersecurity" practice groups whose attorneys advised clients about managing risks associated with data security and the aftermath of data exfiltrations by cybercriminals.

Today, with an estimated 70 percent of all data being generated by individuals (often related to those individuals' activities), and with organizations globally expected to lose over 146 billion more data records between 2018 and 2023 if current cybersecurity tools are not improved,[4] the number of cybersecurity lawsuits is not expected to level off anytime soon.

Ransomware Attacks

While data exfiltration lawsuits have remained the bulk of cybersecurity litigation, few were surprised when the plaintiffs' bar began targeting other cyber issues, most recently ransomware attacks, especially those affecting healthcare facilities.

In ransomware, an organization's computer systems are frozen by malicious software attacks until a ransom is paid. Those alleging injury in such cases say that, while frozen, a defendant was unable to effectively deliver critical services, which caused harm and injury. Where the business is in the healthcare field, plaintiffs claim the organization's delivery of patient-related services was adversely affected.

What data exfiltration and ransomware litigation have in common is the access to and security of confidential and private customer data. When commercial and government organizations fail to take adequate steps to control access to that data or maintain the privacy of their customers' data, litigation ensues.

Leaky machine learning models are likewise built on data, often using tens of thousands of personal data records, and businesses that do not take steps to maintain the privacy of that data may also become embroiled in litigation.

Machine Learning and Membership Inference

In their research, sponsored in part by the National Science Foundation and Google, Shmatikov and his colleagues in early 2017 "uncovered multiple privacy and integrity problems in today's [machine learning] pipelines" that could be exploited by adversaries to infer if a particular person's data record was used to train machine learning models.[5]

They describe a healthcare machine learning model that could reveal to an adversary whether or not a certain patient's data record was part of the model's training data.

In another example, a different model trained on location and other data, used to categorize mobile users based on their movement patterns, could reveal by way of query whether a particular user's location data was used.

These scenarios certainly raise alarms from a privacy perspective, and one can imagine other possible instances of machine learning models revealing the kind of personal information to an attacker that might cause harm to individuals (an attack does not necessarily involve a nefarious purpose, either; an attack could come from law enforcement's investigations of individuals).

While actual user data may not be revealed in these attacks, the mere inference that a person's data record was included in a data set used to train a model, what Shmatikov and previous researchers refer to as "membership inference," could cause that person (and possibly the thousands of others whose data records were used) embarrassment and other consequences.

The membership inference problem is not limited to the discriminative classification machine learning models investigated by Shokri et al. More recently, researchers at the University College London reported membership inference in generative models, specifically generative adversarial networks ("GANs").[6] Generative models are used to generate new data from the same underlying distribution associated with a particular training data set.

The new "synthetic" data can be used to enhance an existing data set, often images or video data. Hayes and his colleagues describe synthetic health-related images generated by a generative model that could leak information about an individual's health if the individual's record was used to train the generative model.

In another example, if images from a database of criminals are used to train a face-generation algorithm, membership inference could leak an individual's criminal past.

Possible Membership Inference Causes of Action

Assuming for the sake of argument that a membership inference disclosure of the kind described above becomes legally actionable, it is instructive to consider what businesses facing membership inference lawsuits might expect in terms of statutory and common law causes of action so they can take steps to mitigate problems and avoid contributing more cyber lawsuits to already busy court dockets (and of course avoid leaking confidential and private information).

These causes of actions could include:

- invasion of privacy;
- consumer protection laws;
- unfair trade practices;
- negligence;
- negligent misrepresentation;
- innocent misrepresentation;
- negligent omission;
- breach of warranty; and
- emotional distress, among others.[7]

Negligence

Negligence might be alleged, as it often is in cybersecurity cases, if plaintiff (or class action members) can establish evidence of the following four elements:

- the existence of a legal duty;
- breach of that duty;
- causation; and
- cognizable injury.

Liability might arise where defendant failed to properly safeguard and protect private personal information from unauthorized access, use, and disclosure, where such use and disclosure caused actual money or property loss or the loss of a legally protected interest in the confidentiality and privacy of plaintiff's/members' personal information.

Misrepresentation

Misrepresentation might be alleged if plaintiff/members can establish evidence of a misrepresentation upon which they relied and a pecuniary loss resulting from the reliance of the actionable misrepresentation. Liability under such a claim could arise if, for example, plaintiff's data record has monetary value and a company makes representations about its use of security and data security measures in user agreements, terms of service, and/or privacy policies that turn out to be in error (for example, the company's measures lack robustness and do not prevent an attack on a model that is found to be leaky).

In some cases, actual reliance on statements or omissions may need to be alleged.

State Consumer Protection Laws

State consumer protection laws might also be alleged if plaintiff/members can establish (depending on which state law applies) deceptive misrepresentations or omissions regarding the standard, quality, or grade of a particular good or service that causes harm, such as those that mislead plaintiff/members into believing that their personal private information would be safe upon transmission to defendant when defendant knew of vulnerabilities in its data security systems.

Liability could arise where defendant was deceptive in omitting notice that its machine learning model could reveal to an attacker the fact that plaintiff's/members' data record was used to train the model. In certain situations, plaintiff/members might have to allege with particularity the specific time, place, and content of the misrepresentation or omission if the allegations are based in fraud.

Defenses

For their part, defendants in membership inference cases might challenge plaintiff's/members' lawsuit on a number of fronts. As an initial tactic, defendants might challenge plaintiff's/members' standing on the basis of failing to establish an actual injury caused by the disclosure (inference) of data record used to train a machine learning model.[8]

Defendants might also challenge plaintiff's/members' assertions that an injury is imminent or certainly impending. In data breach cases, defendants might rely on state court decisions that denied standing where injury from a mere potential risk of future identity theft resulting from the loss of personal information was not recognized, which might also apply in a membership inference case.

Defendants might also question whether permission and/or consent was given by a plaintiffs/members for the collection, storage, and use of personal data records. This query would likely involve plaintiff's/members' awareness and acceptance of membership risks when they allowed their data to be used to train a machine learning model.

Defendants would likely examine whether the permission/consent given extended to and was commensurate in scope with the uses of the data records by defendant or others.

Defendants might also consider applicable agreements related to a user's data records that limited plaintiff's/members' choice of forum and which state laws apply, which could affect pleading and proof burdens. Defendants might rely on language in terms of service and other agreements that provide notice of the possibility of external attacks and the risks of leaks and membership inference.

Many other challenges to a plaintiff's/members' allegations could also be explored.

Preventive Measures

Apart from challenging causes of action on their merits, companies should also consider taking other measures like those used by companies in traditional data exfiltration cases. These might include proactively testing their systems (in the case of machine learning models, testing for leakage) and implementing procedures to provide notice of a leaky model.

As Shmatikov and his colleagues suggest, machine learning model developers and MLaaS providers should take into account the risk that their models will leak information about their training data, warn customers about this risk, and "provide more visibility into the model and the methods that can be used to reduce this leakage."

Machine learning companies should account for these foreseeable risks and associated consequences and assess whether the risks are acceptable compared to the benefits received from their models.

Conclusion

If data exfiltration, ransomware, and related cybersecurity litigation are any indication, the plaintiff's bar may one day turn its attention to the leaky machine learning problem. If machine learning model developers and MLaaS providers want to avoid being the target of this attention and the possibility of litigation, they should not delay taking reasonable steps to mitigate the leaky machine learning model problem.

Notes

* Brian Wm. Higgins is an Intellectual Property & Technology partner at Blank Rome LLP, working with clients to strategically protect, enforce, and defend their intellectual property rights. He may be reached at higgins@blankrome.com.

[1] M. Andreessen, *Why Software is Eating the World,* Wall Street Journal (Aug. 20, 2011).

[2] https://www.cs.cornell.edu/~shmat/.

[3] Privacy Rights Clearinghouse—Data Breaches (available from https://www.privacyrights.org/data-breaches) (accessed Aug. 27, 2018).

[4] Juniper Research, https://www.juniperresearch.com/home.

[5] *See* R. Shokri et al., *Membership Inference Attacks Against Machine Learning Models,* Proceedings of the 38th IEEE Symposium on Security and Privacy (2017).

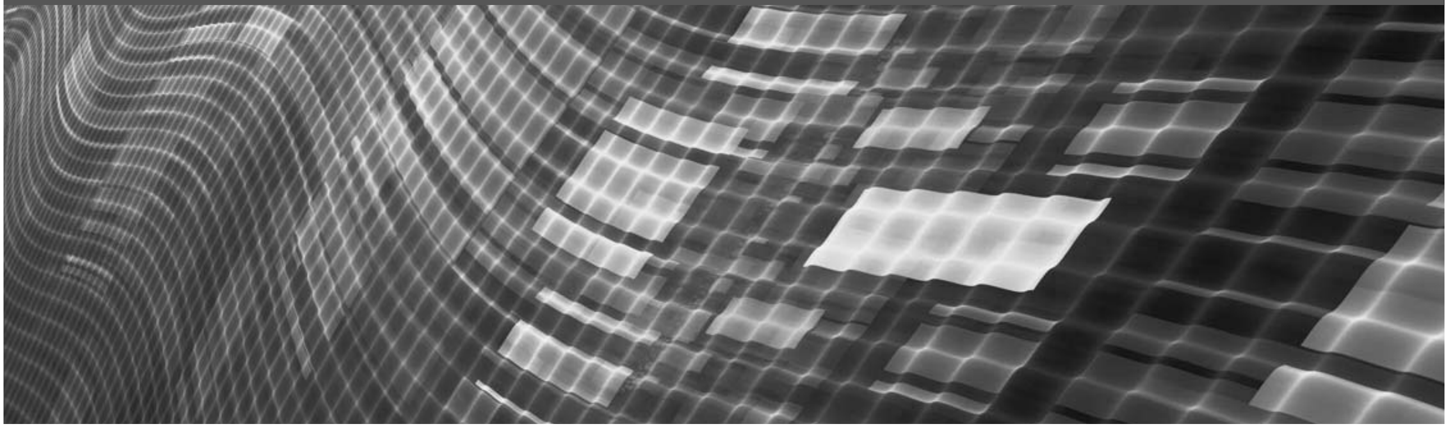
[6] J. Hayes et al*., LOGAN: Membership Inference Attacks Against Generative Models,* Proceedings on Privacy Enhancing Technologies, Vol. 1 (2019) (available on arXiv; Aug. 21, 2018).

[7] *See, e.g., Sony Gaming Networks & Cust. Data Sec. Breach Lit.*, 996 F.Supp. 2d 942 (S.D. Cal 2014) (evaluating data exfiltration causes of action).

[8] *See In re Science App. Intern. Corp. Backup Tape Data,* 45 F. Supp. 3d 14 (D.D.C. 2014) (considering "when, exactly, the loss or theft of something as abstract as data becomes a concrete injury").

BLANKROME

Blockchain Technology & Digital Currencies



NOVEMBER 2018 • NO. 7

SEC Exerts Extraterritorial Jurisdiction over Securities Dealer Accepting Bitcoin

SEC sets its sights on foreign companies and individuals looking to take advantage of America's growing virtual currency market.

On September 27, 2018, the Securities and Exchange Commission ("SEC") filed a complaint in the District Court for the District of Columbia against 1Pool LTD ("1Broker"), a company registered in the Republic of the Marshall Islands, and its CEO, Patrick Brunner, a resident of Austria. The complaint alleges multiple securities law violations in connection with the sale of security-based swaps as "contracts for difference," or "CFDs," to investors over the internet and around the globe. 1Broker sought to take advantage of the growing number of crypto-investors and exclusively accepted investments, and made payments to its investors in, Bitcoin. 1Broker attracted investors who could now spend their Bitcoin on more traditional investments, which caught the SEC's attention.

In its complaint, the SEC alleges that 1Broker sold security-based swaps on its platform to U.S. customers without monitoring the discretionary investment thresholds required by the federal securities laws, that the defendants failed to transact security-based swaps on a registered national exchange, and failed to properly register as a security-based swaps dealer. The SEC has implicated the court's long arm jurisdiction to 1Broker's trading website for actions 1Broker conducted outside of the United States that affected U.S. customers. Because the website was publicly available to U.S. investors, 1Broker and the individual defendants are subject to suit in the United States because they made use of "instruments of transportation or communication in interstate commerce or of the mails to offer to sell, offer to buy or purchase or sell [securities]" in the United States.

In a parallel action, the Commodity Futures Trading Commission ("CFTC") announced charges against 1Broker arising from similar conduct.

For more information, please contact:

Michelle Ann Gitlitz
212.885.5068 | mgitlitz@blankrome.com

Gregory P. Cronin
212.885.5156 | gcronin@blankrome.com

Legaltech news

Vermont Continues Its Blockchain Play: A Look Inside the State's New Legislation

The bill, which became effective on July 1, is designed to stimulate economic development in Vermont through the promotion of blockchain technology.

By **Melissa Palat Murawsky, Kathy E. Herman, and Michelle Ann Gitlitz, Blank Rome** | September 13, 2018

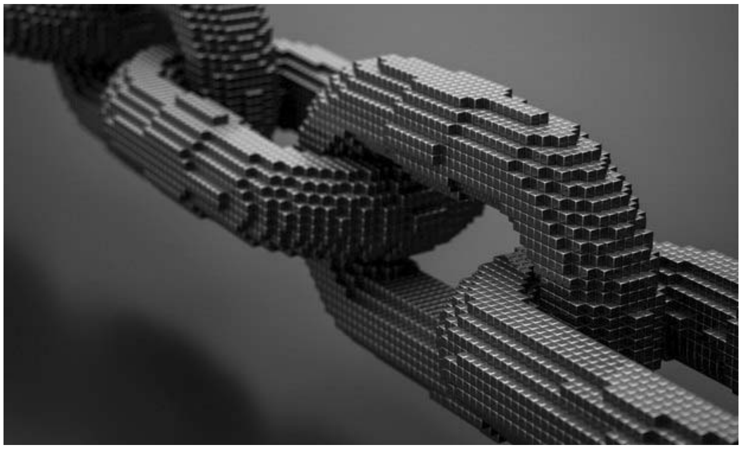


Photo: Shutterstock

On May 30, 2018, Vermont Governor Phil Scott signed into law Senate Bill 269: An Act Related to Blockchain Business Development, which became effective on July 1. The Act is designed to stimulate economic development in Vermont through the promotion of blockchain technology. In passing the Act, Vermont joins the limited ranks of other states that have legislatively recognized the potential of blockchain technology to innovate and spur economic opportunity. We anticipate that other states will follow suit and adopt their own version of blockchain-friendly legislation.

While blockchain may be most widely known as the technology underlying cryptocurrencies, it is, at its core, a system of recording and confirming transactions through a decentralized, shared ledger or database. The decentralized verification ability of blockchain provides for greater security and the fact that the ledgers are immutable creates widespread opportunities for the application of blockchain in many contexts other than just cryptocurrencies.

The Act positions Vermont as an attractive environment for blockchain companies by, among other things, authorizing the creation of a new type of business entity—a blockchain-based limited liability company, or a "BBLLC," for limited liability companies that utilize blockchain technology for a material portion of their business activities. Pursuant to the Act, a BBLLC is allowed to customize its governance structure, in whole or in part and as it sees fit, given its own particular business and technology, through blockchain technology. More specifically, a BBLLC may adopt any reasonable algorithms that it chooses to validate records, as well as requirements, processes, and procedures for conducting its operations, and select the blockchain technology that it will use.

To become a BBLLC, an entity must specify in its articles of organization that it has elected to become a BBLLC, and it must include in its operating agreement a summary of its mission and purpose. The BBLLC must also include in its operating agreement certain decisions regarding such items as access and permission protocols. These provisions include whether the BBLLC's blockchain will be fully or partially decentralized or fully or partially public or private; the extent of a participant's access to information and read and write permissions; how the BBLLC will respond to system security breaches or other unauthorized actions affecting the blockchain technology's integrity; and the rights and obligations of each participant group within the BBLLC. The operating agreement must also set forth voting procedures, which may include smart contracts—that is, whether there will be software code stored on the blockchain that will execute a transaction automatically when certain conditions are met.

The Act also directs Vermont's Department of Financial Regulation to review the potential application of blockchain technology to the insurance and banking industries; to consider areas for potential adoption of blockchain technology; to identify any regulatory changes needed for blockchain technology to have a positive impact on those local industries; and to submit a report of its findings.

Further, the Act allows Vermont's Agency of Commerce and Community Development, together with the Department of Financial Regulation, and representatives from academia and private sector businesses, to organize and hold a fintech summit to, among other matters, explore opportunities to promote blockchain technology in Vermont's state government, private sector, and high schools, colleges, and universities. The Act also requires the agency of Commerce and Community Development to incorporate into one or more of its economic development marketing and business support programs, events, and activities: opportunities to promote blockchain technology in the private sector; legal and regulatory mechanisms that enable and promote the adoption of blockchain and financial technology in Vermont; and educational and workforce training opportunities in blockchain technology, financial technology, and related areas.

Finally, the Act creates another new type of business entity—a personal information protection company, or a "PIPC." PIPCs are businesses organized for the primary purpose of providing personal information protection services to consumers. "Personal information" is defined by the Act as data capable of being associated with a particular natural person, such as gender identification; birth information; marital status; citizenship and nationality; biometric records; government identification designations; and personal, educational, and financial histories. The Act regulates the conduct of these companies, and establishes that any PIPC that accepts personal information pursuant to a written agreement to provide personal information protection services now has a statutory fiduciary responsibility to the consumer in that context. The Act also requires PIPCs to adopt and maintain a comprehensive information security program (that may include the use of blockchain technology) to protect personal information.

This is not the first time that Vermont has passed innovative blockchain legislation. They began establishing a progressive stance on blockchain with the passage of House Bill 868, which was signed into law by former governor Peter Shumlin on June 2, 2016. The act establishes any fact, record or document that is properly verified on the blockchain as admissible in a court of law under Vermont's rules of evidence. Governor Phil Scott first signed into law House bill 182 on May 4, 2017, which defined virtual currency under Vermont's money transmitter laws, establishing digital currencies as "permissible investments," in Vermont under certain circumstances Moreover, the Vermont blockchain initiative progressed when Senate bill 135 was signed into law the following month, on June 8, 2017.

As other state legislatures recognize the potential economic benefits of blockchain, it is likely that they will also enact legislation designed to bring more of the developing blockchain industry to their respective jurisdictions. Vermont may also take additional steps to continue to make the state more hospitable to blockchain development, such as initiatives to make blockchain entities tax advantaged within the state. It remains to be seen whether these anticipated blockchain-friendly laws of other states will follow the same model as Vermont, or will spur greater legislative creativity. In either event, blockchain companies will be served well by paying attention to what happens next.

Melissa Murawsky, Partner in the Corporate practice, focuses her practice on securities and corporate law. She serves a wide range of clients, including those in the manufacturing, insurance, technology, and retail industries. Kathy Herman is an Associate in Blank Rome's Corporate practice. She maintains a practice focused on *providing strategic advice and counsel to companies, management and entrepreneurs on a broad variety of business issues. Michelle Gitlitz serves as Chair of the General Litigation Practice Group and Co-Chair of Blank Rome's Blockchain Technology and Digital Currencies Group. Ms. Gitlitz represents corporations, investment companies, and funds on a wide range of issues, including corporate, regulatory, and litigation matters.*

BLANKROME

Fund and Investment Management

OCTOBER 2018 • NO. 4

Regulatory Update and Recent SEC Actions

REGULATORY UPDATES

The U.S. Securities and Exchange Commission ("SEC") Rule Permitting Electronic Delivery of Materials as Default Method Faces Backlash
On August 8, 2018, the Coalition for Paper Options ("CPO"), which represents consumer groups and print communication companies, petitioned the U.S. Court of Appeals for the D.C. Circuit to review SEC Rule 30e-3, which was adopted on June 4, 2018. Rule 30e-3 permits mutual funds to make annual and semi-annual performance reports and other required materials accessible online free of charge to the public and allows funds to mail a paper notice of the same to investors. In order to rely on Rule 30e-3, funds must make (1) shareholder reports, (2) the most recent prior report, and (3) the last fiscal year's quarterly holdings report available online while abiding by certain format and location requirements. CPO's petition argued that Rule 30e-3 is "arbitrary and capricious and otherwise not in accordance with the law, and does not promote protection of consumers or efficiency, competition, and capital formation." CPO also argued that making electronic delivery the default distribution method imposes a burden on certain investors. "It also imposes hardship on seniors, Americans in rural areas, and other investors least able to manage the change, while opening the door to new phishing scams and cybersecurity threats," said CPO executive director John Runyan. The petitioners are also seeking a permanent injunction against the SEC's ability to implement and enforce the rule.

SEC to Review Denial of Applications for Bitcoin-Based Exchange-Traded Funds
On August 22, 2018, the SEC Staff rejected applications for nine bitcoin-based exchange-traded funds ("ETFs") due to their noncompliance with the Exchange Act of 1934. The Staff had previously rejected a bitcoin ETF

application due, in part, to concerns over manipulation of bitcoin. The SEC's decision to review the Staff's disapproval orders for the nine bitcoin ETFs is consistent with the SEC's option to review actions delegated to its Staff. While it is unclear what the SEC will decide, the willingness to review its Staff's decision provides hope to the cryptocurrency community that a bitcoin ETF may be permitted in the future.

ENFORCEMENT ACTIONS AND CASES

SEC v. Temenos Advisory, Inc. (Case No. 3:18-cv-001190, D. Conn.)

On July 18, 2018, the SEC filed a complaint against George L. Taylor and his Connecticut-based firm Temenos Advisory Inc. ("Temenos") for allegedly collecting hidden commissions and related financial incentives in luring clients toward making high-risk investments in four private companies. According to the SEC's complaint, Taylor and Temenos obscured the risks from clients by inflating the profitability of the illiquid private placements as they were paid in commissions as unregistered broker-dealers. Before 2014, Taylor and Temenos typically invested client money in mutual funds, ETFs and variable annuities and charged clients a standard fee for those services. However, from 2014 through 2017, the SEC claims that Temenos began aggressively recommending investments in four private companies and invested over $19 million into these companies' securities. Additionally, the SEC complaint states that Taylor and Temenos neglected to conduct basic due diligence on the four companies and never told clients about the financial stability of the four companies, their business prospects, or about the sustainability of the investments. The SEC alleges that Taylor and Temenos were offered finder's fees between 2.5 percent and 10 percent of the investments secured, which were inherently illegal because Taylor and Temenos were not registered broker-dealers. Taylor and Temenos were sued for two claims of investment adviser fraud—one count of acting as an unregistered broker-dealer and one count of failing to abide by written policies—and procedures as mandated by securities law.

> ***"Through their conduct, Temenos and Taylor violated the fiduciary duty that every investment adviser owes to its clients and prospective clients—to put client interests first, to deal with clients with the utmost honesty, to disclose all conflicts or potential conflicts of interest, and to use reasonable care in providing investment advice," the SEC said. "Instead, defendants ignored their clients' interests and biased their investment advice to put money in their own pockets."***

In Re BlackRock Mutual Funds ("BlackRock") Advisory Fee Litigation (Case No. 3:14-cv-01165)

On August 20, 2018, plaintiff shareholders of two BlackRock mutual funds alleged in New Jersey district court that they paid excessive advisory fees of approximately $280 million per year relative to the amount of fees that other funds receive for providing similar advisory services. The complaint states that these fees were not a result of an arm's-length negotiation, but rather in connection to the value of the services received, including portfolio management, legal and compliance monitoring, regulatory reporting, securities valuation, recordkeeping, and proxy voting coordination. BlackRock Advisors LLC, BlackRock Investment Management LLC, and BlackRock International Ltd. (collectively, the defendants) responded that the fees were justified, and are allegedly less than the industry medium. Defendants stated that the service fees are determined by the percentage of assets under management ("AUM"), and court records showed that BlackRock's AUM increased from $23 billion to $58 billion between 2007 and 2013. The complaint was originally filed in February 2014, alleging that BlackRock breached its fiduciary duty by receiving highly-disproportionate service fees relative to the services being offered and that the fees bore "no reasonable relationship to the value of the services provided" to the shareholders and, in doing so, the defendants failed to appropriately share the benefits of scale with the shareholders as well.

SEC v. Robbins et al. (Case No. 1:18-cv-23368, S.D. Fla.)

On August 20, 2018, the SEC alleged that defendants Barry M. Kornfeld, Ferne Kornfeld, Lynette M. Robbins, Andrew G. Costa, Albert D. Klager, and four of their companies sold to more than 1,600 retail investors over $243 million worth of unregistered securities of bankrupt Woodbridge Group of Companies LLC ("Woodbridge"). Woodbridge went out of business last year after it was caught by the SEC for running a $1.2 billion Ponzi scheme. According to the SEC's complaint, the defendants, who were not registered broker-dealers, allegedly earned millions in commissions on the sales of Woodbridge securities as unauthorized brokers. The SEC claims that the defendants marketed Woodbridge as "safe and secure" investments and sought potential investors at a Florida university retirement and income planning class they taught. The SEC is seeking the return of ill gotten gains plus interest and penalties against the defendants and their companies. Separately, Robbins and her company Knowles Systems settled with the SEC by returning one million dollars without admitting or denying the allegations, and also paid $100,000 in civil fines.

In the Matter of Merrill Lynch Pierce Fenner & Smith Inc. ("Merrill Lynch") (Case No. 3-18651)

On August 20, 2018, Merrill Lynch agreed to pay $8.9 million to the SEC in connection with claims that it failed to disclose a conflict of interest to customers with respect to offering certain investment products managed by a third-party adviser. On August 20, 2018, the due diligence unit at Merrill Lynch's Global Wealth and Retirement Solutions concluded that various investment products should have been terminated after a subsidiary of an anonymous foreign multinational bank convinced Merrill Lynch's governance committee to retain the investments. Over 1,500 of Merrill Lynch's retail advisory clients invested roughly $575 million into the products prior to their termination. Merrill Lynch, without admitting or denying the SEC's allegations, agreed to be censured and to disgorge over four million dollars in fees plus prejudgment interest totaling over $800,000.

Jalbert v. SEC (Case No. 1:17-cv-12103, D. Mass.)

In October 2017, Craig Jalbert filed a class action lawsuit against the SEC in his capacity as a trustee of the "F2 Liquidating Trust" challenging whether disgorgement was an available remedy for the SEC, which had allegedly illegally collected approximately $15 billion in disgorgement penalties. On August 22, 2018, U.S. District Court Judge F. Dennis Saylor IV ruled that the U.S. Supreme Court's decision in *Kokesh v. SEC* did not prohibit the SEC from collecting disgorgement payments. In the suit, F-Squared Investment Management LLC's ("F-Squared") liquidation trustee argued that the *Kokesh* ruling prohibited the SEC from "double dipping" by collecting both disgorgements and penalties in civil or administrative enforcement actions. In 2017, *Kokesh* held that the SEC is subject to a five-year statute of limitations with respect to collecting civil penalties. F-Squared claimed that the SEC used disgorgement as a means to tack on additional penalties including a $30 million penalty that F-Squared agreed to pay prior to filing for bankruptcy, while the SEC argued that *Kokesh* merely instituted a five-year statute of limitations on the agency's ability to obtain ill-gotten gains. Judge Saylor ruled that the SEC retains the right to collect disgorgement under the 1990 Penny Stock Reform Act stating, "an action, suit or proceeding for the enforcement of any civil fine, penalty, or forfeiture, pecuniary or otherwise" must be "commenced within five years from the date when the claim first accrued.” Additionally, Judge Saylor ruled that *Kokesh* “did not change the ability of the SEC to collect disgorgement in civil enforcement proceedings and “that opinion says nothing about the application of disgorgement in administrative proceedings.”

Attorneys have been questioning the SEC’s disgorgement power based on a footnote written by Justice Sonia Sotomayor in the Kokesh decision, which said, “Nothing in this opinion should be interpreted as an opinion on whether courts possess authority to order disgorgement in SEC enforcement proceedings or on whether courts have properly applied disgorgement principles in this context.” Judge Saylor dismissed the Jalbert dispute because the SEC had the authority to enter a disgorgement order at the time, and F-Squared had entered into a binding settlement with the SEC in which it expressly waived judicial review.

***Obeslo et al. v. Great-West Capital Management* (“Great-West”) (Case No. 16-230, D. Colo.)**

On September 12, 2018, U.S. District Judge Christine Arguello rejected plaintiff investors’ argument accusing Colorado investment advisor Great-West of charging the investors excessive management fees, and thereby breaching its fiduciary duty to the investors under the U.S. Investment Company Act of 1940 (the “40 Act”). Under the 40 Act, an advisor is in breach of its fiduciary duty if its compensation is disproportionate to the services it provides. The investors argued that they had standing to sue for fees charged in connection with 63 mutual funds managed by Great West because the funds were issued in a single series, even though the investors owned only 19 of the funds. Judge Arguello disagreed, ruling that the investors may only sue over the funds they actually own. “For all practical purposes, each fund in a series is a separate mutual fund. Plaintiffs may pursue claims only on behalf of funds in which they are invested,” Judge Arguello stated.

Thomas R. Westle and Michelle Ann Gitlitz would like to thank Brandon R. Einstein and Adam R. Seiden for their contributions to this update.

For more information, please contact:

Thomas R. Westle
212.885.5239 | twestle@blankrome.com

Michelle Ann Gitlitz
212.885.5068 | mgitlitz@blankrome.com

Notice: The purpose of this update is to identify select developments that may be of interest to readers. The information contained herein is abridged and summarized from various sources, the accuracy and completeness of which cannot be assured. This update should not be construed as legal advice or opinion, and is not a substitute for the advice of counsel.

Topic III

Crowdfunding and Initial Coin Offerings

“ROYALTY FINANCING”: THE NEW, NEW THING IN VENTURE CAPITAL

By Cliff Ennico

“I have a successful retail business that I want to take online with a killer website and a social media marketing campaign on Facebook and Twitter.

The problem, of course, is money. I need to raise $100,000 to build the website and launch the campaign, but am having trouble finding the money. My business has strong cash flows, but has never officially shown a profit. There aren’t a whole lot of tangible assets in this business, and I don’t have tons of equity in my home, so most local banks won’t even talk to me. And I’m not really willing to give up 50% of my company to a venture capitalist.

Are there any other options out there I may have overlooked?”

You sound like a near-perfect candidate for the hottest new development in venture capital: so-called “royalty financing”.

The concept of “royalty financing” has been around for a long time. Basically, the idea is this: someone lends you money (in this case, $100,000), but instead of a fixed interest rate, you agree to pay the lender a percentage of your gross sales (not net profits) each month – 2% to 6% is customary. The royalty payments may continue for a specified time period (generally three to five years), or until the lender has received all of their money back plus a 20% return on their investment (in this case, $120,000 in total payout). Once the time period expires or the desired return has been achieved, the loan is considered fully paid and you stop making the royalty payments each month.

Most, but not all, royalty financings also involve an “equity kicker” – the lender takes a piece of equity in your company (or, more commonly, a warrant to acquire shares) on top of the royalty payments each month. So if your company grows and becomes profitable, the lender will be entitled to a piece of your “upside” growth.

Why is royalty financing gaining traction right now? Basically, in a difficult economy where most entrepreneurial companies are struggling to break even and taking longer to become profitable, lenders to growing businesses have become tired of waiting for their money. Your business is not currently showing a profit, and it will have to do so before legally you can pay any sort of dividend or distribution to your investors. That may take years. Because most “royalty financings” are structured as loans, they do not run afoul of state laws requiring that dividends be paid only out of “earnings and profits”. And your investors see a steady return on their investment each month.

There are several advantages to both parties in royalty financing. Because the lender is getting money back every month, it is taking less of a risk than it would making a traditional equity investment in your company. If your business grows rapidly, so will the lender’s monthly royalty payments, meaning they will get their return on investment a Heck of a lot faster than they would buying stock in your company. Accordingly, a royalty investor may be willing to accept a smaller amount of equity as its “kicker” than it would in a traditional equity investment -- this leaves you the entrepreneur with more equity in your business, and less dilution for you and your business partners.

Also, the default provisions in royalty loans are usually much less onerous than in traditional bank financings. While most royalty loans require a minimum royalty payment each month, many investors will allow you to pay less than the minimum royalty for two, sometimes even three, consecutive months without putting you into default. Many royalty investors will also insist on converting their loan into straight equity in your company, rather than foreclosing on their loan, if you default in your royalty payments.

There are, however, some disadvantages to royalty financing. If your company is not demonstrating strong, steady and predictable cash flows each month, you are not likely to interest an investor in royalty financing. Also, royalty financing deprives you of some much-needed cash each month that you otherwise would pay for rent, payroll, business expenses, not to mention your compensation as owner of the business. Most investors insist that their royalty payment be made "on top" – i.e. before you pay other expenses – which may leave you cash-strapped at the end of the month if business unexpectedly turns down.

Having said that, though, for businesses with few tangible assets and zero profits, it may be the only type of financing you can get in a difficult market.

So where do you find royalty investors? A number of firms are setting up venture funds built entirely around the royalty financing concept. Among those are Arctaris Capital Partners L.P. in Waltham, Massachusetts (www.arctaris.com); Cypress Growth Capital LLC in Dallas, Texas (www.cypressgrowthcapital.com); Revenue Loan LLC in Seattle, Washington (www.revenueloan.com); and Noventi Ventures in Menlo Park, California (www.noventivc.com).

But as royalty financing becomes more popular, even local venture firms will be testing the waters. There's no harm in asking . . .

Cliff Ennico (crennico@gmail.com) is a syndicated columnist, author and former host of the PBS television series "Money Hunt." This column is no substitute for legal, tax or financial advice, which can be furnished only by a qualified

professional licensed in your state. To find out more about Cliff Ennico and other Creators Syndicate writers and cartoonists, visit our Web page at www.creators.com. COPYRIGHT 2011 CLIFFORD R. ENNICO. DISTRIBUTED BY CREATORS.COM

TAX EXEMPT AND
GOVERNMENT ENTITIES
DIVISION

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

OCT 1 2008

MEMORANDUM FOR DIRECTOR, EMPLOYEE PLANS EXAMINATIONS
DIRECTOR, EMPLOYEE PLANS RULINGS & AGREEMENTS

FROM: Michael D. Julianelle, Director, Employee Plans, SE:T:EP

SUBJECT: Guidelines regarding rollovers as business start-ups

Recently, personnel in our examination and determination letter functions have identified a retirement plan design that appears to operate primarily to transact in employer stock, resulting in the avoidance of taxes otherwise applicable to distributions from tax-deferred accumulation accounts.

Although we do not believe that the form of all of these transactions may be challenged as non-compliant *per se*, issues such as those described within this memorandum should be developed on a case-by-case basis. Those cases currently in process or held in suspense should be worked within the context of these guidelines. Please cascade this memorandum to your managers and technical employee staff as appropriate.

EXECUTIVE SUMMARY

A version of a qualified plan is being marketed as a means for prospective business owners to access accumulated tax-deferred retirement funds, without paying applicable distribution taxes, in order to cover new business start-up costs. For purposes of this memorandum, these arrangements are known as Rollovers as Business Startups, or ROBS. While ROBS would otherwise serve legitimate tax and business planning needs, they are questionable in that they may serve solely to enable one individual's exchange of tax-deferred assets for currently available funds, by using a qualified plan and its investment in employer stock as a medium. This may avoid distribution taxes otherwise assessable on this exchange. Although a variety of business activity has been examined, an attribute common to this design is the assignment of newly created enterprise stock into a qualified plan as consideration for these transferred funds, the valuation of which may be questionable.

BACKGROUND

Employee Plans first identified ROBS provisions giving rise to these transactions through our regular compliance processes, including determination letter submissions and later project examination activity. They are proprietary defined contribution plans, generally established in the form of profit sharing plans coupled with a cash or deferred arrangement (CODA). Several different promoters have crafted variations on this design, but the elements of each are sufficiently similar that they can be addressed generally.

Although ROBS arrangements may operate as profit sharing plans, their primary purpose appears to be to provide funding for the establishment of a business or franchise. They are designed to allow a newly created business entity to retrieve available tax-exempt accumulation funds from its principal in exchange for its capital stock, simultaneously avoiding all otherwise imposable distribution income and excise taxes that would ordinarily apply to the transaction.

The typical ROBS customer is an individual seeking to start up a personal business, and having accumulated tax-deferred investment funds, usually in the form of a defined contribution account created under a prior employer's plan.[1] From our review of open cases, franchises are often the business form of choice, and this design is marketed as a funding method on various internet sites.

After client engagement, the practitioner-promoter apparently advises the individual to create a C-corporation. A number of corporate shares may be created, but they are not issued. After incorporation is complete, the practitioner installs a qualified profit sharing plan, sponsored by the shell corporate entity. The plan document used is generally a "pre-approved" specimen, but is usually supplemented with a single amendment. This amendment generally exists as either a stand-alone amendment or a tack-on addition to a qualified plan adoption agreement, and consists of a one paragraph provision to permit the plan to invest plan assets attributable to rollover accounts up to 100% in employer securities.

The individual then executes either a rollover or direct trustee-to-trustee transfer of the proceeds from the available tax-deferred investment account into this newly created plan. At this point, the prior account is usually liquidated; all proceeds are parked in a rollover account held in trust under the shell corporation's plan.

The amendment provision is then acted on immediately, and the individual directs the corporation to issue and then exchange all of its capital stock into its qualified plan in exchange for the proceeds held in the rollover account. The corporate shares, now held as plan assets, are valued and booked equal to the value of available account proceeds.

[1] At the time the ROBS transaction is executed, some of these amounts may remain as deferred separated accounts held under a prior plan trust, and some appear to have been rolled over into a "conduit IRA", which was a common utility for individual retirement arrangements prior to the expanded portability provisions enacted by the Economic Growth Tax Relief and Reconciliation Act of 2001.

Usually, after the exchange of stock is complete, no other plan participant will ever receive any ability to invest in employer stock. In some ROBS versions, the provision permitting the stock investment is eliminated immediately after exchange, by means of a second amendment that serves to prospectively redact that provision. In all versions, the exchange fully allocates all of the stock to the rollover sub-account created for the benefit of the individual, and no further allocations of stock to future participants are permitted.

A ROBS transaction therefore takes the form of the following sequential steps:

- An individual establishes a shell corporation sponsoring an associated and purportedly qualified retirement plan. At this point, the corporation has no employees, assets or business operations, and may not even have a contribution to capital to create shareholder equity.

- The plan document provides that all participants may invest the entirety of their account balances in employer stock.

- The individual becomes the only employee of the shell corporation and the only participant in the plan. Note that at this point, there is still no ownership or shareholder equity interest.

- The individual then executes a rollover or direct trustee-to-trustee transfer of available funds from a prior qualified plan or personal IRA into the newly created qualified plan. These available funds might be any assets previously accumulated under the individual's prior employer's qualified plan, or under a conduit IRA which itself was created from these amounts. Note that at this point, because assets have been moved from one tax-exempt accumulation vehicle to another, all assessable income or excise taxes otherwise applicable to the distribution have been avoided[2].

- The sole participant in the plan then directs investment of his or her account balance into a purchase of employer stock. The employer stock is valued to reflect the amount of plan assets that the taxpayer wishes to access.

- The individual then uses the transferred funds to purchase a franchise or begin some other form of business enterprise. Note that all otherwise assessable taxes on a distribution from the prior tax-deferred accumulation account are avoided.

[2] Distributions from tax-deferred accumulation accounts would generally be taxed under IRC § 72, which specifies treatment for various forms of annuity or non-annuity payments. In general, a single sum distribution would be taxed as ordinary income, at the individual's effective tax rate. Of particular concern here, the distribution would generally also be subject to the 10% "premature distribution" penalty provided by IRC § 72(t), unless the individual was at least 59½ years old on the transaction date, or met one of the other limited statutory exceptions. ROBS transactions effectively avoid all § 72 concerns.

- After the business is established, the plan may be amended to prohibit further investments in employer stock. This amendment may be unnecessary, because all stock is fully allocated. As a result, only the original individual benefits from this investment option. Future employees and plan participants will not be entitled to invest in employer stock.

- A portion of the proceeds of the stock transaction may be remitted back to the promoter, in the form of a professional fee. This may be either a direct payment from plan to promoter, or an indirect payment, where gross proceeds are transferred to the individual and some amount of his gross wealth is then returned to promoter.

PROCEDURAL DEVELOPMENT OF CASES

Employee Plans has received numerous alerts from practitioners regarding the promotion of this scheme in the marketplace. Questions regarding the legitimacy of ROBS-type transactions have been posed to the Service at various employee benefits and practitioner conferences.[3]

We have currently identified 9 promoters of this transaction. Most are actively promoting the use of ROBS at seminars that are held to assist individuals purchase business franchises. A referral to the Lead Development Center (LDC) has already been made and an LDC Investigator has been assigned.

We have also coordinated our consideration of ROBS plans with the Department of Labor (DOL). As will be noted later, the transfer of enterprise stock within a ROBS arrangement could raise ERISA Title I prohibited transaction issues. Although our coordination efforts are not yet finalized, they remain ongoing.

Additionally, SB/SE has reviewed several returns of employers who have engaged in ROBS transactions. Their examinations have largely started with a review of business tax returns, and then moved on to a review of promoter activity.

Determination Letter Contacts

EP Determinations identified numerous determination letter submissions for taxpayer adoptions of these plans. Most are filed by a named representative who is also a pre-approved document platform provider. Since the type of plan used for this promotion is a prototype plan with a minor amendment that permits the investment in employer securities, we have issued some favorable determination letters for these plans. We are also likely to receive many more submissions within the two-year EGTRRA pre-approved adoption window created by Announcement 2008-23, 2008-14 I.R.B. 731.

[3] For example, a fact pattern describing a ROBS arrangement was presented at the American Bar Association's 2003 Joint Committee on Employee Benefits "Q&A". See *http://www.abanet.org/jceb/2003/qa03irs.pdf,* question 9 therein.

A major promoter was first identified through our determination letter program as the sponsor of a pre-approved prototype, or "M&P", which has been approved by the Service under our pre-approved opinion letter program. This document is then marketed to clients, and is ultimately adopted by employers by the execution of adoption agreements. The base document from which client plans are administered is thus a pre-approved M&P specimen supplied by the provider which was reviewed and approved by the Service with a favorable opinion letter.

Because of the unique rules regarding scope of reliance applicable to M&P adopters, a modification of an M&P generally requires submission for a determination letter application as an individually designed plan. Thus, we are confident that the determination letter database will eventually hold a registry of most, if not all, of this promoter's clients, once the two-year window closes on April 30, 2010.

Current Examination Contacts

We have examined a number of these plans – having opened a specific examination project on them based off referrals from our determination letter program – and found significant disqualifying operational defects in most. For example, employees in some arrangements have not been notified of the existence of the plan, do not enter the plan or receive contributions or allocable shares of employer stock. Additionally, we have identified that plan assets are either not valued or are valued with threadbare appraisals. Required annual reports for some plans have not been filed. In several situations, we have also found that the business entity created from the ROBS exchange has either not survived, or used the resultant assets on personal, non-business purchases.

Again, considering business activity that occurs, it is likely that many ROBS plans did in fact file returns that are currently in place on RICS. The amount of the asset transfer is likely to exceed the minimum $100,000 that would otherwise eliminate filing of Form 5500EZ, *Annual Return/Report of Employee Benefit Plan.*[4]

In those cases, however, where the appropriate Form 5500 or 5500EZ was not filed, issues may arise as to the proper way to correct a failure to file. For example, issues may arise due to DOL's mandate for electronic filing beginning with the 2009 plan year and the resulting limitations on filing paper returns. It is anticipated that additional guidelines will be issued to address these situations.

[4] Form 5500 filing is triggered by when the value of trust assets reaches a specified level. See Treas. Reg.§ 301.6058-1(a)(1), et seq. Note that Section 1103(a) of the Pension Protection Act of 2006, Pub. L. 109-280, increased the amount of assets required for filing by one-participant plans from $100,000 to $250,000 effective for plan years beginning after December 31, 2006. Note also that Form 5500EZ will be replaced with Form 5500-SF, beginning with year 2009 filings.

PRIMARY ISSUES RAISED:

The two primary issues raised by ROBS arrangements are (1) violations of nondiscrimination requirements, in that benefits may not satisfy the benefits, rights and features test of Treas. Reg. § 1.401(a)(4)-4, and (2) prohibited transactions, due to deficient valuations of stock.

Benefits, Rights & Features Discrimination

Because ROBS transactions generally benefit only the principal involved with setting up a business, and do not enable rank-and-file employees to acquire employer stock, we believe that some of these plans violate the anti-discrimination provisions of the Code and Regulations, on a case-by-case basis.

IRC § 401(a)(4) provides that, under a qualified retirement plan, contributions or benefits provided under the plan must not discriminate in favor of highly compensated employees (HCEs).

IRC § 414(q)(1)(A) provides that an HCE is defined as either (1) a 5% owner, defined under the attribution rules of § 318, or (2) receives compensation over $80,000 (indexed, and subject to a "top-paid group" election by the employer.)

IRC § 318(a)(2)(B)(i) precludes attribution of stock owned by a plan described in § 401(a) to any participant in the plan for whom the stock is held for the benefit of, in trust.

Treas. Reg. § 1.401(a)(4)-1(b)(2) provides that in order to satisfy § 401(a)(4), either the contributions or the benefits under a plan must be nondiscriminatory in amount.

Treas. Reg. § 1.401(a)(4)-4(e)(3) provides that the plan's benefits, rights and features (BRFs) are tested to see if they are nondiscriminatory in effect. BRF testing considerations can arise in many forms, including as here, the right to make investments in employer securities.

Treas. Reg. § 1.401(a)(4)-4(b)(1) indicates that whether any given BRF is "currently available" (i.e. nondiscriminatory in result) should be tested under the nondiscriminatory classification test used for coverage testing. Further, Reg. § 1.401(a)(4)-4(c) provides that a BRF must also be "effectively available" to non-highly compensated employees (NHCEs), on the basis of all facts and circumstances.

Treas. Reg. § 1.401(a)(4)-5 provides that whether the timing of a plan amendment or series of plan amendments has the effect of discriminating specifically in favor of HCEs involves a facts and circumstances determination.

In a typical ROBS arrangement, there may not be any individual who meets the statutory HCE definition. At the time when rollover funds are used to purchase employer stock, the stock acquires identity as a trust asset and is not attributed to the individual participant. Compensation paid then becomes the determining factor in resolving HCE status questions.[5]

In most of our cases, the amount of compensation being paid to the individual who starts-up the business is ostensibly below the IRC § 414(q)(1)(B) dollar limit, at least for initial years. While this may leave open the question as to whether true compensation being paid to the individual is actually higher than reported compensation, absent a personal tax review of the individual no one may receive compensation at or above the HCE indexed dollar limit.

Even if the ROBS initiator is an HCE, in many of our cases, there are no other employees in the initial year of the transaction or for some number of future years thereafter. Therefore, as no finding regarding discrimination can be made in absence of NHCEs in the transaction year, the current availability testing standard for plan BRFs is satisfied. This does not, however, signify that the effective availability standard is similarly resolved.

Effective availability testing requires a facts and circumstances determination regarding whether a plan feature benefits NHCEs. This determination requires consideration of factors or conditions precedent that must be satisfied in order to accrue a benefit, including timing elements and whether the transaction was structured to intentionally avoid BRF testing issues. Furthermore, Treas. Reg. § 1.401(a)(4)-5 requires consideration as to whether the timing of plan amendments serves to preclude other NHCEs from receiving stock allocations.

Given that ROBS arrangements are designed to take advantage of a one-time only stock offering, the investment feature generally would not satisfy the effectively available benefit requirement. The issue of discrimination arises because the plan is designed in a manner that the BRF will never be available to any NHCEs. For this reason, ROBS cases should be developed for discrimination issues whenever a given plan covers both HCEs and NHCEs, and no extension of the stock investment option is afforded to NHCEs.

Prohibited Transactions – Valuation of Stock

In all ROBS arrangements, an aspiring entrepreneur creates capital stock for the purpose of exchanging it for tax-deferred accumulation assets. The value of the stock is set as the value of the available assets. An appraisal may be created to substantiate this value, but it is often devoid of supportive analysis. We find this may create a prohibited transaction, depending on true enterprise value.

[5] In several of our examined cases, the transaction did not exactly follow the sequential series of steps outlined earlier. Instead, the principal received shares of the shell corporation prior to the sale back to the plan. This timing made the principal a 100% owner for a short period of time. In such a case, HCE status is conferred on start-up, perhaps creating an imminent BRF testing issue. This might also raise related prohibited transaction concerns.

IRC § 4975(a) imposes a tax on a prohibited transaction equal to 15% of the amount involved in the transaction. IRC § 4975(b) imposes a tax equal to 100% of the amount involved in any case where a prohibited transaction is not corrected within the taxable period, as defined at § 4975(f).

IRC § 4975(c)(1)(A) defines a prohibited transaction as a sale, exchange or lease of any property between a plan and a disqualified person.

IRC § 4975(e)(1)(F) defines a plan as any trust, plan, account or annuity that is exempt from tax under § 501(a), or was ever determined by the Secretary to be so exempt.

IRC § 4975(e)(2)(C) defines a disqualified person as an employer, any of whose employees are covered by the plan.

IRC § 4975(e)(2)(E)(i) defines a disqualified person as an owner, direct or indirect, of 50% or more of the combined voting power of all classes of stock entitled to vote or the total value of shares of all classes of stock of a corporation which is an employer described in § 4975(e)(2)(C).

IRC § 4975(d)(13) provides an exemption from prohibited transaction consideration for any transaction which is exempt from ERISA § 406, by reason of ERISA § 408(e), which addresses certain transactions involving employer stock.

IRC § 4975(f)(2) defines the taxable period as the period beginning with the date on which the prohibited transaction occurs and ending on the earlier of the dates on which a) a notice of deficiency with respect to the tax imposed by § 6212(a) is mailed, b) the date on which the tax imposed by § 4975(a) is assessed, or c) the date on which correction of the prohibited transaction is completed.

IRC § 4975(f)(5) defines correction as the undoing of the transaction, to the extent possible, such that the plan is restored to a financial position not worse than it would have been absent the transaction.

ERISA § 408(e), and ERISA Reg. § 2550.408e promulgated thereunder, provides an exemption from ERISA § 406 for acquisitions or sales of qualifying employer securities, subject to a requirement that the acquisition or sale must be for "adequate consideration." Except in the case of a "marketable obligation", adequate consideration for this purpose means a price not less favorable than the price determined under ERISA § 3(18).

ERISA § 3(18) provides in relevant part that, in the case of an asset other than a security for which there is no generally recognized market, adequate consideration means the fair market value of the asset as determined in good faith by the trustee or named fiduciary pursuant to the terms of the plan and in accordance with regulations.

An exchange of company stock between the plan and its employer-sponsor would be a prohibited transaction, unless the requirements of ERISA § 408(e) are met. Therefore, valuation of the capitalization of the new company is a relevant issue. Since the company is new, there could be a question of whether it is indeed worth the value of the tax-deferred assets for which it was exchanged. If the transaction has not been for adequate consideration, it would have to be corrected, for example, by the corporation's redemption of the stock from the plan and replacing it with cash equal to its fair market value, plus an additional interest factor for lost plan earnings.

A valuation-related prohibited transaction issue may arise where the start-up enterprise does not actually "start-up." Here, the start-up entity might record "cash" as its only asset, without any real attempt to secure, for example, a franchise license, property, plant and equipment or other assets necessary to start a bona fide business. The valuation ostensibly legitimizing the exchange is unsupported.

Many examiners have been provided with a single sheet of paper, signed by a purported valuation specialist. This appraisal "certifies" that the value of the enterprise stock is a sum certain, the amount of which approximates the amount of available proceeds from the individual's tax deferred retirement account.

These appraisals are questionable. Because the valuation usually approximates available funds, consideration needs to be given to whether inherent value in the plan-acquired entity actually exists. The lack of a bona fide appraisal raises a question as to whether the entire exchange is a prohibited transaction.[6]

Prohibited Transactions – Promoter Fees

In the case where the plan purchases the stock of the employer, and the employer immediately pays professional fees to the promoter out of the proceeds, prohibited transactions may occur.

IRC § 4975(c)(1)(E) prohibits a fiduciary from dealing with the assets of the plan in his own interest or his own account.

IRC § 4975(e)(3) defines a fiduciary as any person who exercises any discretionary authority or control, renders investment advice for a fee, or has any discretionary authority or responsibility in the administration of the plan.

Treas. Reg. § 54.4975-9(c) defines when a person would be providing investment advice as defined in § 4975(e)(3)(B).

ERISA Reg. § 2510-3.21(c) further clarifies the meaning of the term "investment advice." Under that regulation, a person is deemed to render investment advice if such person renders advice to the plan as to the value of securities or other property, or makes a recommendation as to the advisability of investing in, purchasing, or selling securities or other property and such person either directly or indirectly has discretionary authority or control, whether or not pursuant to an agreement, arrangement or understanding, with respect to purchasing or selling securities or other property for the plan. The advice would have to be rendered on a regular basis to the plan pursuant to a mutual agreement, arrangement or understanding, written or

[6] We note that deficient valuations can also raise qualification issues. See e.g. Rev. Rul. 80-155, 1980-1 CB 84.

otherwise, between such person and the plan or a fiduciary with respect to the plan, that such services will serve as a primary basis for investment decisions with respect to plan assets, and that such person will render individualized investment advice to the plan based on the particular needs of the plan regarding such matters as, among other things, investment policies or strategy, overall portfolio composition, or diversification of plan investments.[7]

If the promoter meets these requirements, his status may rise to that of plan fiduciary. Where a fiduciary directly receives a remit-back from the plan of a portion of tax-deferred accumulation assets, this payment may be a violation of IRC § 4975(c)(1)(E). Essentially, plan assets are being transferred in exchange for services and investment advice. Specialists will need to ascertain whether this is discernable from the facts presented on their examination, and whether the requirements of Treas. Reg. § 54.4975-9(c) have been met.

Note that IRC § 4975(f)(1) provides that where more than one person is liable for prohibited transaction excise taxes, all persons are jointly and severally liable for any deficiency. Therefore, assessments against promoters for direct receipt of plan assets may be made even where assessments are proposed against the corporation or individual for invalid appraisal of the underlying stock.[8]

OTHER ISSUES:

Permanency

Because ROBS benefits are designed to be used only once, we have considered whether they are truly a "permanent" retirement program. Permanency is a qualification requirement for all retirement plans.

IRC § 401(a)(1) provides that a trust is established for the purpose of distributing to such employees or their beneficiaries the corpus and income of the fund accumulated by the trust in accordance with such plan.

Treas. Reg. § 1.401-1(b)(1)(ii) provides that a profit sharing plan is established to enable employees or their beneficiaries to participate in the profits of the employer's trade or business, or in the profits of an affiliated employer who is entitled to deduct his contributions to the plan under IRC § 404(a)(3)(B), pursuant to a definite formula for allocating the contributions and for distributing the funds accumulated under the plan.

[7] DOL has taken the position that this definition of fiduciary also applies to investment advice provided to a participant or beneficiary in an individual account plan that allows participants or beneficiaries to direct the investment of their accounts. See ERISA Reg. § 2509.96-1(c).

[8] In an attempt to "insulate" client adopters against prohibited transaction issues, one promoter has apparently created a multiple employer plan within the meaning of IRC § 413(c), with each client adopting-in as a participating employer. Notwithstanding this attempt, the analysis supplied by this memorandum should be applied to these cases.

Treas. Reg. § 1.401-1(b) provides that a qualified plan must be created primarily for the purposes of providing systematic retirement benefits for employees. Treas. Reg. § 1.401-1(b)(2) requires that the plan be a permanent, as distinguished from temporary, arrangement, and provides a general rule that if a plan is discontinued within a few years after its adoption, there is a presumption that it was not intended as a permanent program from its inception, unless business necessity required the discontinuance, termination or partial termination.

Rev. Rul. 69-25, 1969-1 C.B. 113, provides that for purposes of invoking this "business necessity" exception, the necessity must have been unforeseeable when the plan was adopted, and cannot be within the control of the employer.

Consider that business reasons – tax motivated or otherwise – are generally the only reasons why a retirement arrangement is installed. Similarly, they are likely to be the only reason why they are terminated as well. For this reason, permanency is not an area where the Service has aggressively challenged plan terminations or design considerations. Additionally, Regulations address permanency within the context of an entire plan arrangement, not necessarily to a feature within a plan.

Therefore, a plan containing a ROBS arrangement would have to be shown to be non-permanent in its entirety. Many of the ROBS arrangements we have examined also contain a CODA feature. Plans which suffer from permanency failures are generally deficient in that they do not receive substantial and recurring contributions. Because CODA features receive contributions only if participants make contributions, the issue of permanence is resolvable in favor of the employer.

Under the specific facts presented by the cases we have examined, we are unable to find that all ROBS arrangements violate the permanency rule. However, facts of particular cases should be considered on a case-by-case basis.[9]

Exclusive Benefit

As noted earlier, ROBS arrangements typically involve direction of some amount of plan assets to the promoter in payment of professional fees for setting up the transaction. In some cases, the newly created business purchased assets that were essentially personal assets for the benefit of the individual. We considered whether this violates the "exclusive benefit" requirements of the Code.

IRC § 401(a)(2) provides, in relevant part, that a plan is not qualified unless it is impossible, at any time prior to the satisfaction of all liabilities with respect to employees and their beneficiaries, for any part of the corpus or income to be used for or diverted to purposes other than for the exclusive benefit of employees or their beneficiaries.

[9] In fact, as will be noted later, some plans appear to have been established with CODAs that do not receive contributions and may not have been adequately communicated to employees. These plans would not be insulated against permanency issues.

Treas. Reg. § 1.401-1(a)(3)(iv) provides that it must be impossible "under the trust instrument at any time before the satisfaction of all liabilities with respect to employees and their beneficiaries under the trust, for any part of the corpus or income to be used for, or diverted to, purposes other than for the exclusive benefit of the employees or their beneficiaries.

Treas. Reg. § 1.401-2 outlines the specific provisions that a plan must follow to meet the exclusive benefit rule for purposes of Title II of ERISA. Other applicable exclusive benefit issues are contained in corresponding Title I provisions.

We have reviewed ROBS arrangements to determine whether they are truly for the exclusive benefit of employees. The facts unique to each of our ROBS cases are disparate as to the eventual disposition of tax deferred accumulation assets. In a few cases, these assets wound up purchasing personal assets, like recreational vehicles. But in many, if not most of the transactions, the assets were in fact used to purchase legitimate business or franchises, plus attendant start-up costs. Courts have generally held that whether a Title II exclusive benefit violation has occurred largely depends on whether benefits to third parties are not merely an incidental side effect of an investment of trust assets, but are instead a major purpose of the investment.

Therefore, we believe that the typical ROBS design does not violate the exclusive benefit requirement in form.[10] Examiners will need to develop specific operational issues, such as where trust assets were used to pay purely non-business expenses prior to pursuing exclusive benefit violations.[11]

Plan not communicated to employees

In some cases, we have found that the existence of the plan is not communicated to people hired after the newly created business is up and running. "Participants", as identified on employee census information provided to our examiners, are not even aware that they merit this classification. If this can be established, the plan may be in violation of Treas. Reg. § 1.401-1(a)(2), requiring that it be a definite, written program communicated to employees. In some cases, employees may not reach participation status into the plan on their required entry dates, causing the plan to fail IRC § 410(a) requirements.

Inactivity in cash or deferred arrangement

A large number of reviewed plans contain election provisions in the adoption agreement to utilize a CODA. Often, low number of participants actually chose to make salary reduction contributions. However, many of our examiners found this issue and raised it, and usually received a response that the CODA was "inactive." In fact, many of these

[10] However, we are aware of arrangements in which the individual transferring tax-deferred assets into the plan is not an employee, participant or owner, such as where the arrangement is used to set up a business for a spouse. Such a transfer might be one where the exclusive benefit issue is properly raised.

[11] As a reminder, exclusive benefit revocation cases must be submitted for technical advice consideration under established procedures within each business unit.

plans have provisions describing a CODA feature, including applicable elections in the employer's signed adoption agreement. There being no such thing as an "inactive" CODA, examiners should consider whether all the procedures for allowing employees to participate in the CODA were followed, whether new employees just chose not to defer, or whether employees were not even offered salary reduction elections. If it is established that employees were not permitted to make elective deferrals, the plan would violate IRC § 401(k)(2)(D) in that it did not permit eligible employees to elect salary deferral contributions.[12]

COMPLETION AND MOVEMENT OF CASES

Determination Letter Contacts

We have specifically considered whether the form of the plan, as presented, is entitled to a favorable determination letter ruling. There is no inherent violation in the form of a plan containing a ROBS arrangement that would otherwise prevent a favorable ruling. The issues described herein are inherently operational, and beyond the scope of a determination letter ruling. Accordingly, determination letter applications for plans with ROBS features can be reviewed and approved as appropriate. However, we will monitor the volume of approval letters issued to these plans in a manner similar to those issued to IRC § 412(i) arrangements. Current procedures for these notifications, including review by EP Determinations Quality Assurance, are to be followed for ROBS determination letter submissions.

Open Examination Cases

Open examination cases should be worked within the context of these guidelines. Cases presenting prohibited transaction issues should be worked under existing procedures for processing delinquent returns in agreed cases, and under unagreed procedures for all other circumstances, including appropriate referral to and coordination with DOL. Cases in which BRF discrimination is an issue should be processed first under the appropriate Employee Plans Compliance Resolution System (EPCRS) correction program. If EPCRS is not appropriate or available, then unagreed qualification procedures should be followed.

Statute of Limitation Concerns

For BRF discrimination and other disqualification cases, normal control procedures for protection of applicable statutes of limitation on trust and related taxable returns should be followed. This may involve converting non-calendar year plans, and annualizing income in accordance with IRC § 645(a). Related returns should be protected, generally for the individual and employer sponsor only.

[12] Also, to the extent that a CODA supports the permanency of a plan, that support expires if in fact the CODA is not in fact communicated to employees.

Similar procedures are also applicable for prohibited transaction cases, however, specialists are cautioned that one other consideration may block pursuing deficiency determinations for these cases.

IRC § 6501(a) provides that the amount of any tax, including those imposed by Chapter 43 (such as IRC § 4975) may be assessed within three years after the "return" was filed.

IRC § 6501(l) further provides that, for this purpose, the term "return" means the annual Form 5500 series return required to be filed by plan/trust for the year in which the act occurred. Therefore, in most instances, the statute of limitation to make a prohibited transaction assessment on a ROBS transaction begins with the filing of Form 5500 for the year in which the stock transaction is executed.

IRC § 6501(e)(3) provides, however, that if this information return does not adequately disclose the existence of this transaction, the ordinary limitation period on assessment is extended to six years. Adequacy of disclosure is largely a facts and circumstances determination, developed through judicial interpretation.[13]

Prohibited transactions are classifiable into either "discrete" one-time transactions, or "continuous" recurring transactions.[14] ROBS arrangements fall into the former. In a discrete transaction, a taxable event occurs in the initial or "source" year when the prohibited exchange of stock occurs, and is deemed to be carried forward into later taxable periods until corrected.[15]

The Service's position with respect to administering the limitation period on assessment applicable to discrete transactions is that the source year must be open in order to make any assessment in the source or any later year. If this source year is barred by elapse of the relevant limitation statute, no excise tax deficiency may be assessed. Given the length of time that has elapsed since many of these transactions first were created and the time involved moving these cases through our determination letter and audit cycle processes, it is likely that the three-year limitation period has either elapsed or is imminent for most of these transactions.

Therefore, ROBS prohibited transaction cases are likely to require a determination as to whether a six-year statute is open, under a failure to make adequate disclosure of the existence of the transaction in the source year. For this purpose, coordination with Area Counsel will be required.[16] Specialists are reminded that statutes are to be protected, and assessments perfected, against the correct parties. Where the 3-year limitation period is open, it should be protected in lieu of relying on a 6-year period.

[13] See e.g. *Janpol v. Commissioner*, 102 T.C. 499 (1994)

[14] Note that these terms are not derived from statute or regulation, but are administrative creations.

[15] Unlike a continuous transaction, in which the taxable amount involved accumulates with a future interest factor in the manner known as "pyramiding", a discrete transaction's taxable amount is simply replicated forward in later years.

[16] Peter Gavagan, of Northeast Area Counsel, will coordinate application of 6-year statutes of limitation to open ROBS examination cases.

CONCLUSION

ROBS transactions may violate law in several regards. First, this scheme might create a prohibited transaction between the plan and its sponsor. At the time of the exchange between plan assets and newly-minted employer stock, the value of the capitalization of the entity is equivalent to the value of all plan assets, when in reality, the entity may be valueless and asset-less for an indefinite period of time. Additionally, this scheme may not satisfy the benefits, rights and features requirement of the Regulations. The primary utility of the arrangement may only be available the business's principal individual.

Specific facts will need to be evaluated on a case by case basis in order to make a proper determination as to whether these plans operationally comply with established law and guidance. Technical advice requests may be submitted after consultation with group managers. For this reason, employee plans specialists are directed to resolve open ROBS cases as described herein.[17]

[17] As additional reference material, see IRM § 4.72.8, *Valuation of Assets,* and § 4.72. ., *Prohibited Transactions.*

Crowdfunding, Coin Offerings and Other Cutting-Edge Financing Techniques for Startup Ventures

Cliff Ennico
Law Offices of Clifford R. Ennico
2490 Black Rock Turnpike # 354
Fairfield, Connecticut 06825-2400
Tel.: (203) 254 1727
Fax: (203) 254 8195
E-Mail: crennico@gmail.com

Disclaimers

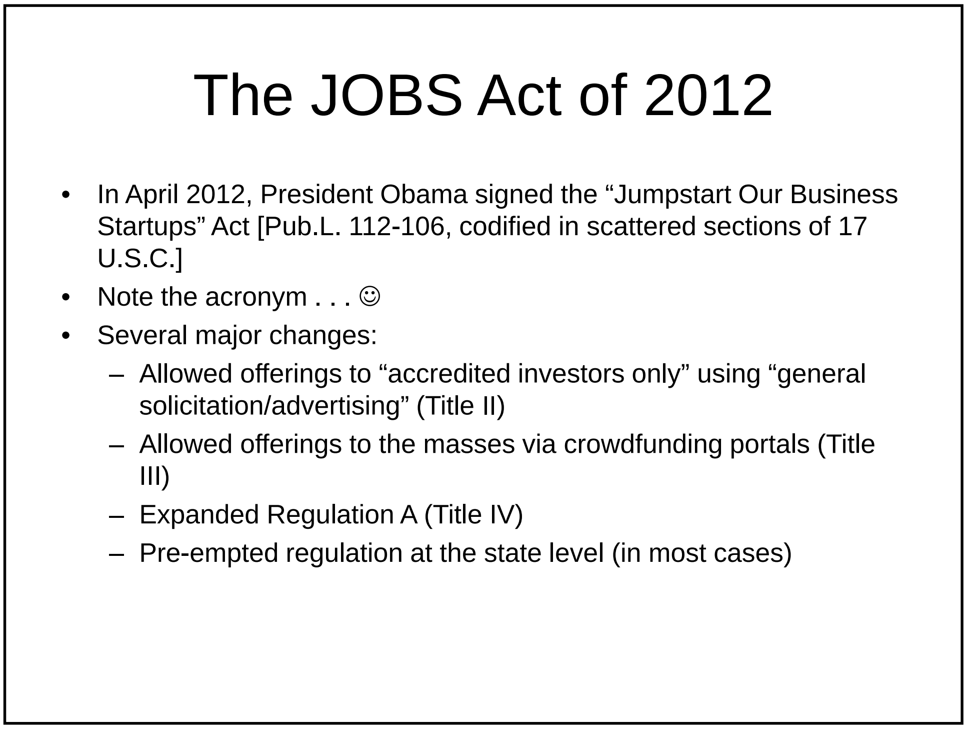
- Views expressed in this program are Cliff's own, and do not reflect the views of NYSBA, or indeed anyone else.
- Legal and tax information presented in this program SHOULD NOT be relied upon as legal or tax advice, which can only be given by a lawyer, accountant or other professional licensed to practice in your state.
- *Tax-Related Disclaimer: To comply with the requirements of Treasury Department Circular 230, which provides regulations governing certain conduct of U.S. tax professionals giving written advice with respect to U.S. tax matters, please be aware that any U.S. federal tax advice contained in this communication (including any attachments) is not intended to be used and cannot be used, by you or any other person for the purpose of (i) avoiding penalties that may be imposed under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any tax-related matter addressed herein.*

What is Crowdfunding?

- Raising money from “the masses”
- Base of the Statue of Liberty (1885)
- For a “project” of some type, such as:
  - An invention;
  - A book or other creative project;
  - A surgical procedure not covered by insurance
- Launch a “campaign” on a crowdfunding portal such as kickstarter.com, Indiegogo.com
- Then promote it aggressively on social media

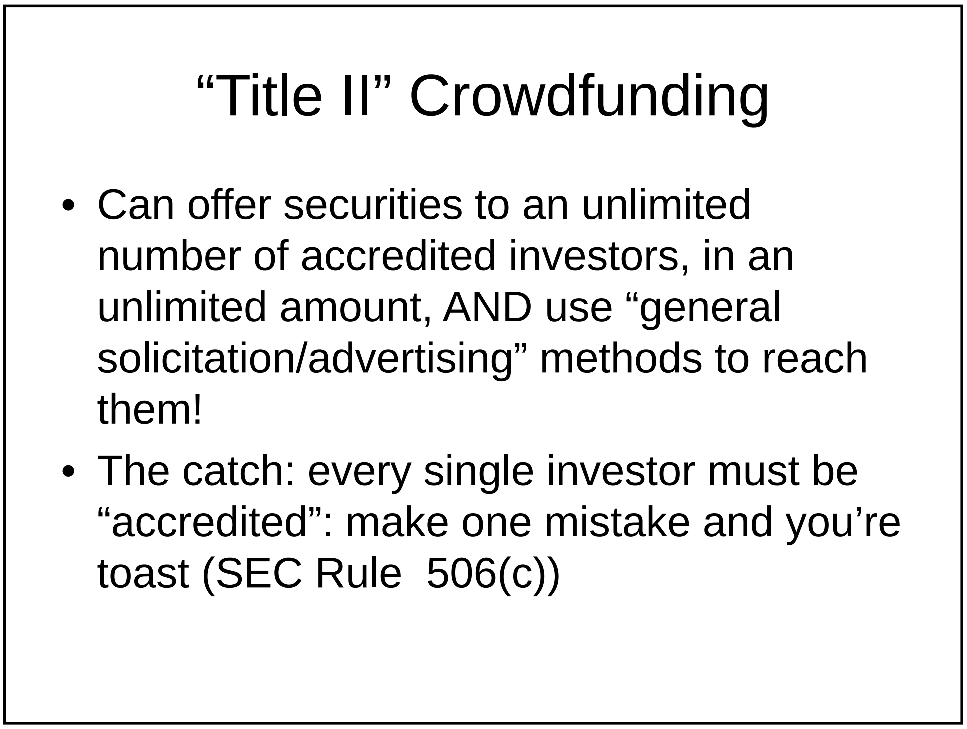
Types of Crowdfunding

- In “project crowdfunding,” investor gets something in return (eventually)
- In “gift crowdfunding,” investor gets a warm, fuzzy feeling (and maybe a tax deduction)
- Beginning May 16, 2016, there is “equity crowdfunding” – raising money for your business, and offering stock or debt in return!



The JOBS Act of 2012

- In April 2012, President Obama signed the “Jumpstart Our Business Startups” Act [Pub.L. 112-106, codified in scattered sections of 17 U.S.C.]
- Note the acronym . . . ☺
- Several major changes:
  - Allowed offerings to “accredited investors only” using “general solicitation/advertising” (Title II)
  - Allowed offerings to the masses via crowdfunding portals (Title III)
  - Expanded Regulation A (Title IV)
  - Pre-empted regulation at the state level (in most cases)



“Title II” Crowdfunding

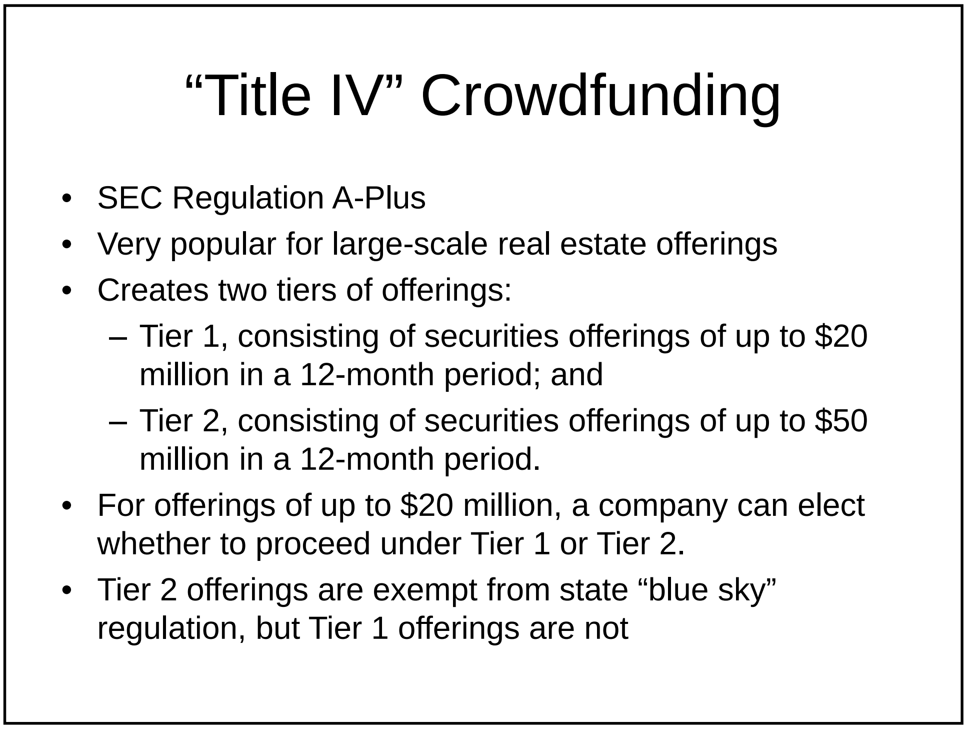
- Can offer securities to an unlimited number of accredited investors, in an unlimited amount, AND use “general solicitation/advertising” methods to reach them!
- The catch: every single investor must be “accredited”: make one mistake and you’re toast (SEC Rule 506(c))

“Title III” Crowdfunding

- Taking the “friends and family” offering to a new level*
  - ideal for B2C companies with compelling products/services/stories
- Issuers can raise up to $1,070,000 over a rolling 12-month period via specialized gatekeepers called “crowdfunding portals”**
  - All communications with advertisers, and all advertising, must be conducted through the portal or in a “tombstone” ad under Rule 204(b)***
- Little or no regulation at the state level
- People other than “accredited investors” can participate, as long as they don’t invest more than:
  - $2,200 or 5% of their net worth or annual income (whichever is greater) in crowdfunded offerings each year if their net worth and annual income are both less than $107,000;
  - 10% of their net worth or annual income (whichever is less) in crowdfunded offerings if either their net worth and annual income is $107,000 or more;
  - $107,000 total in crowdfunded offerings***.

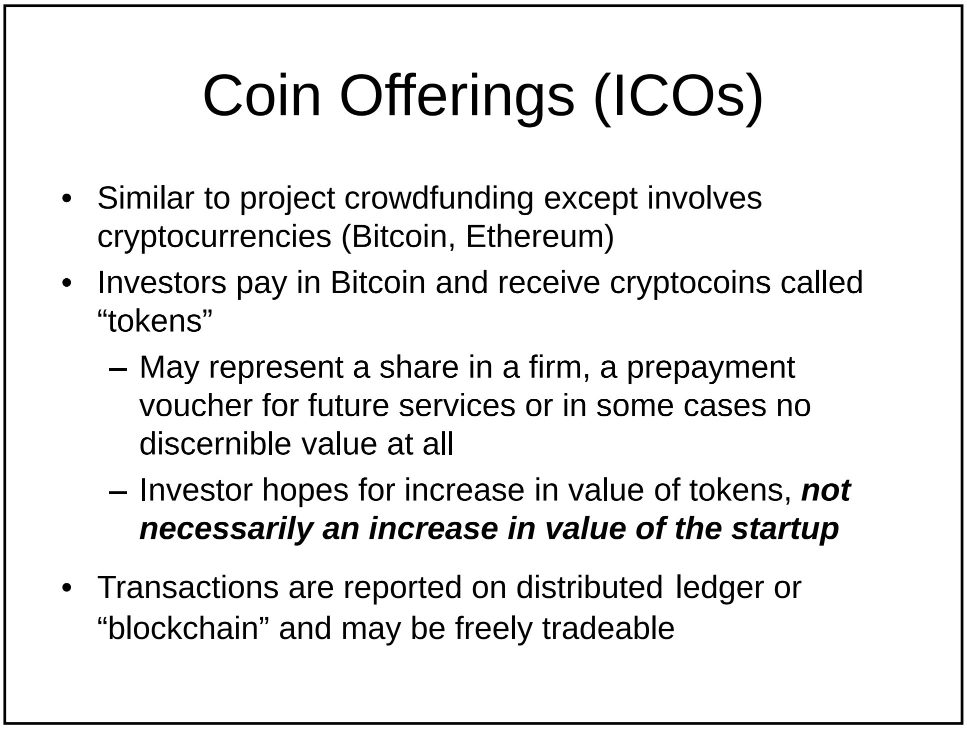
“Title III” Crowdfunding

- Recent Developments*
  - More than 1,300 offerings since May 2016
  - Heavy participation by consumer products, liquor, and entertainment startups, NOT so much tech companies
  - Offerings are for: nonvoting equity, SAFEs (Simple Agreement For Future Equity) and revenue sharing notes
  - Success rate (achieving target offering amount) is in 30% to 35% range
  - Portal commissions range from 3% to 12% of offering amount
  - In November 2016, FINRA shut down the Virginia-based crowdfunding portal uFundingPortal (UFP) for allegedly allowing 16 issuers to sell securities through the portal without having filed the requisite paperwork with the SEC



“Title IV” Crowdfunding

- SEC Regulation A-Plus
- Very popular for large-scale real estate offerings
- Creates two tiers of offerings:
  - Tier 1, consisting of securities offerings of up to $20 million in a 12-month period; and
  - Tier 2, consisting of securities offerings of up to $50 million in a 12-month period.
- For offerings of up to $20 million, a company can elect whether to proceed under Tier 1 or Tier 2.
- Tier 2 offerings are exempt from state “blue sky” regulation, but Tier 1 offerings are not



Coin Offerings (ICOs)

- Similar to project crowdfunding except involves cryptocurrencies (Bitcoin, Ethereum)
- Investors pay in Bitcoin and receive cryptocoins called “tokens”
  - May represent a share in a firm, a prepayment voucher for future services or in some cases no discernible value at all
  - Investor hopes for increase in value of tokens, ***not necessarily an increase in value of the startup***
- Transactions are reported on distributed ledger or “blockchain” and may be freely tradeable

Coin Offerings (ICOs)

- Most issuers are extremely early stage or “concept” companies.
- Startup creates a plan or whitepaper which states what the project is about, what need(s) the project will fulfill upon completion, how much money is needed to undertake the venture, how much of the virtual tokens the pioneers of the project will keep for themselves, what type of money is accepted, and how long the ICO campaign will run for.
- Needs to be “crystal clear” as to what the token represents and what rights holders of tokens have.

Regulation of ICOs****

- Banned in China and South Korea
- Mexico: must be authorized in advance
- US and UK regulators say the tokens may be “securities”*
- In the US, will apply the *Howey* test**
- If a security, ICO offerings must be registered with SEC or qualify for one of the Regulation D exemptions***

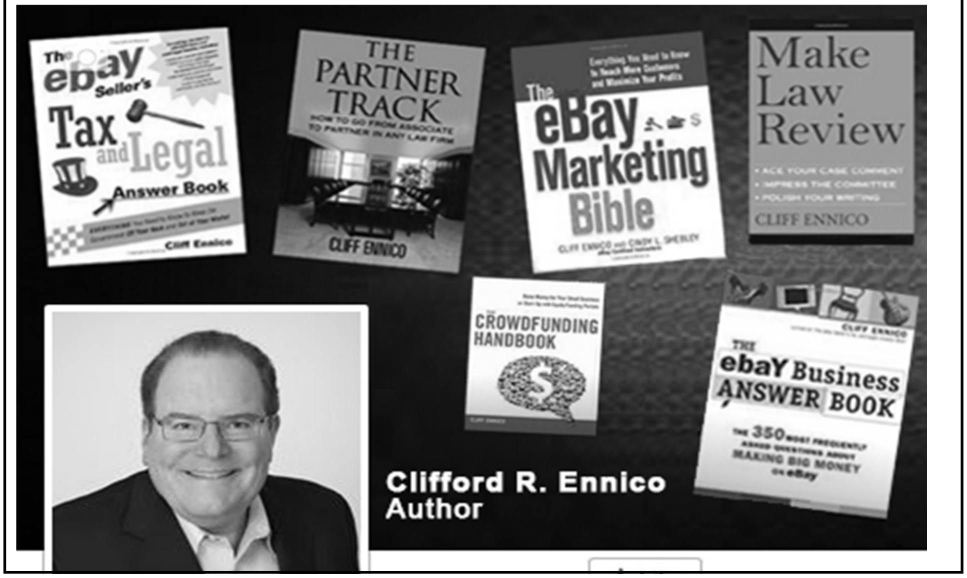
Some Points to Ponder

- Can an ICO offering be effected as a private placement to accredited investors only with “general solicitation and advertising” under SEC Rule 506(c)?
- Can larger ICO offerings be made under Regulation A-Plus?

“Cutting Edge” Financing Tools

- Royalty Financing (see materials)
- SAFE (simple agreement for future equity)
- The “equity linked note”
  - No interest, holder gets % of increase in underlying equity x “participation rate”
  - http://en.wikipedia.org/wiki/Equity-linked_note
- The Rollover as Business Startup (ROBS)
  - Form a C corporation, then roll over 401(k) into corporation’s profit sharing plan
  - http://en.wikipedia.org/wiki/Rollovers_as_Business_Start-Ups

Thank You!


The ebay Seller's Tax and Legal Answer Book
Cliff Ennico
THE PARTNER TRACK
HOW TO GO FROM ASSOCIATE TO PARTNER IN ANY LAW FIRM
CLIFF ENNICO
The eBay Marketing Bible
CLIFF ENNICO and CINDY L. SHEBLEY
Make Law Review
• ACE YOUR CASE COMMENT
• IMPRESS THE COMMITTEE
• POLISH YOUR WRITING
CLIFF ENNICO
THE CROWDFUNDING HANDBOOK
CLIFF ENNICO
THE ebaY Business ANSWER BOOK
THE 350 MOST FREQUENTLY ASKED QUESTIONS ABOUT MAKING BIG MONEY ON eBay
Clifford R. Ennico
Author

Questions and Answers

Cliff Ennico
Attorney, Author and Columnist
2490 Black Rock Turnpike, # 354
Fairfield, Connecticut 06825-2400, U.S.A.
Tel.: (203) 254 1727
Fax: (203) 254 8195
e-Mail: crennico@gmail.com
www.succeedinginyourbusiness.com

Topic IV

Artificial Intelligence and the Law

ARTIFICIAL INTELLIGENCE AND THE FUTURE OF LEGAL PRACTICE

BY GARY E. MARCHANT

The alarming headlines and predictions of artificial intelligence (AI) replacing lawyers have no doubt created discomfort for many attorneys already anxious about the future of their profession: "Rise of the Robolawyers." "Here Come the Robot Lawyers." "Why Hire a Lawyer? Machines Are Cheaper." "Armies of Expensive Lawyers, Replaced by Cheaper Software." "Law Firm Bosses Envision Watson-Type Computers Replacing Young Lawyers." "Why Lawyers and Other Industries Will Become Obsolete. You Should Stop Practicing Law Now and Find Another Profession." And so on.

Despite these dire headlines, AI will fortunately not replace most lawyers' jobs, at least in the short term. One in-depth study of the legal field estimated that AI would reduce lawyers' billing hours by only 13 percent over the next five years.[1] Other estimates are a little less sanguine, but still not projecting a catastrophic impact on attorney employment. A database on the effect of automation on over 800 professions created by McKinsey & Company found that 23 percent of the average attorney's job could be replaced by robots.[2] A study by Deloitte estimated that 100,000 legal jobs will be eliminated by automation in the United Kingdom by 2025.[3] And last year JPMorgan used an AI computer program to replace 360,000 billable hours of attorney work, with one report of this development observing that "[t]he software reviews documents in seconds, is less error-prone and never asks for vacation."[4]

***Gary E. Marchant, PhD** (gary.marchant@asu.edu) is a Regents' Professor, Lincoln Professor of Emerging Technologies, Law & Ethics, and Faculty Director of the Center for Law, Science & Innovation at the Sandra Day O'Connor College of Law at Arizona State University. His teaching and research interests focus on the governance of emerging technologies. Prior to his joining the faculty of ASU in 1999, Professor Marchant was a partner at Kirkland & Ellis in Washington, D.C.*

As with many new technologies, there is a cycle of hype at the outset that creates inflated expectations, even though the long-term implications of that technology may be profound and enormous. As Bill Gates perceptively noted in his book *The Road Ahead*, "[w]e always overestimate the change that will occur in the next two years and underestimate the change that will occur in the next ten."[5] Right now, AI in the practice of law is more of an opportunity than a threat, with early adopters providing more efficient and cost-effective legal services to an expanding portfolio of existing and potential clients.

The use of AI in law will thus be an evolution, not a revolution.[6] But make no mistake, AI is already transforming virtually every business and activity that attorneys deal with, some more quickly and dramatically than others, and the legal profession will not be spared from this disruptive change. Incorporation of AI into a law firm's systems and operations is a gradual, learning process, so early adopters will have a major advantage over firms that lag in adopting the technology. The lawyers, law firms, and businesses that do not get on the AI bandwagon will increasingly be left behind, and eventually displaced. As a recent *ABA Journal* cover story explained, "Artificial intelligence is changing the way lawyers think, the way they do business and the way they interact with clients. Artificial intelligence is more than legal technology. It is the next great hope that will revolutionize the legal profession."[7]

What Is Artificial Intelligence

At its simplest, AI is the development and use of computer programs that perform tasks that normally require human intelligence. At this time and for the foreseeable future, current AI capabilities only permit computers to approach, achieve, or exceed certain but not all human cognitive functions. While some researchers are working on developing computers that can match or eclipse the human mind, sometimes referred to as "general intelligence" or "superintelligence,"[8] such an achievement is likely decades away. That is why important legal skills based on human judgment, inference, common sense, interpersonal skills, and experience will remain valuable for the lifetime of any lawyer practicing today.

While AI has many attributes for its many different applications, two are currently most important for legal applications. First, *machine learning* is the capability of computers to teach themselves and learn from experience. This means that the AI can do more than blindly adhere to what it has been programmed to do, but can learn from experience and data to constantly improve its capabilities. This is how Google's Deep Mind system was able to defeat the world's best human Go players. Second, *natural language processing* is the capability of computers to understand the meaning of spoken or written human speech and to apply and integrate that understanding to perform human-like analysis.

AI is rapidly being applied to all major sectors of the economy and society, including medicine, finance, national defense, transportation, manufacturing, the media, arts and entertainment, and social relationships, to name just some. Many of these applications will create new legal issues for lawyers, such as the liability issues of autonomous cars, the legality of lethal autonomous weapons, financial bots that may run afoul of antitrust laws, and the safety of medical robots. But in addition to changing the subject matter that lawyers work on, it will also transform the way lawyers practice their craft.

AI Applications for Legal Practice

AI is rapidly infiltrating the practice of law. A recent survey of managing partners of U.S. law firms with 50 or more lawyers found that over 36 percent of law firms, and over 90 percent of large law firms (>1,000 attorneys), are either currently using or actively exploring use of AI systems in their legal practices.[9] The following summary describes some of the major categories and examples of such applications.

Technology-Assisted Review

Technology-assisted review (TAR) was the first major application of AI in legal practice, using technology solutions to organize, analyze, and search very large and diverse data sets for e-discovery or record-intensive investigations. Going far beyond keyword and Boolean searches, studies show that TAR provides a fifty-fold increase in efficiency in document review than human review.[10] For example, predictive coding is a TAR technique that can be used to train a computer to recognize relevant documents by starting with a "seed set" of documents and providing human feedback; the trained machine can then review large numbers of documents very quickly and accurately, going beyond individual words and focusing on the overall language and context of each document. Numerous vendors now offer TAR products.

Legal Analytics

Legal analytics use big data, algorithms, and AI to make predictions from or detect trends in large data sets. For example, Lex Machina, now owned by LexisNexis, uses legal analytics to predict trends and outcomes in intellectual property litigation, and is now expanding to other types of complex litigation. Wolters Kluwer leverages a massive database of law firm billing records to provide baselines, comparative analysis, and efficiency improvements for in-house counsel and outside law firms on staffing, billing, and timelines for various legal matters. Ravel Law, also recently purchased by LexisNexis, uses legal analytics of judicial opinions to predict how specific judges may decide cases, including providing recommendations on specific precedents and language that may appeal to a given judge. Law professor Daniel Katz and his colleagues have utilized legal analytics and machine learning to create a highly accurate predictive model for the outcome of Supreme Court decisions.[11]

Practice Management Assistants

Many technology companies and law firms are partnering to create programs that can assist with specific practice areas, including transactional and due diligence, bankruptcy, litigation research and preparation, real estate, and many others. Sometimes billed as the first robot lawyer, ROSS is an online research tool using natural language processing powered by IBM Watson that provides legal research and analysis for several different law firms today, and can reportedly read and process over a million legal pages per minute. It was first publicly adopted by the law firm BakerHostetler to assist with its bankruptcy practice, but is now being used by that firm and several others for other practice areas as well. A similar system is RAVN developed in the United Kingdom and first publicly adopted by the law firm Berwin Leighton Paisner in London in 2015 to assist with due diligence in real estate deals by verifying property details against the official public records. According to the law firm attorney in charge of implementation: "once the program has been trained to identify and work with specific variables, it can complete two weeks' work in around two seconds, making [it] over 12 million times quicker than an associate doing the same task manually."[12] Kira is another AI system that has already been adopted by several law firms to assist with automated contract analysis and data extraction and due diligence in mergers and acquisitions.

Legal Bots

Bots are interactive online programs designed to interact with an audience to assist with a specific function or to provide customized answers to the recipient's specific situation. Many law firms are developing bots to assist current or prospective clients in dealing with a legal issue based on their own circumstances and facts. Other groups are developing pro bono legal bots to assist people who may not otherwise have access to the legal system. For example, a Stanford law graduate developed an online chat bot called DoNotPay that has helped over 160,000 people resolve parking tickets, and is now being expanded to help refugees with their legal problems.

Legal Decision Making

AI is enabling judicial decision making in a number of ways. For example, the Wisconsin Supreme Court recently upheld the use of algorithms in criminal sentencing decisions.[13] While such algorithms represent an early use of primitive AI (some may not consider such algorithms AI at all), they open the door to use more sophisticated AI systems in the sentencing process in the future. A number of online dispute resolution tools have or are being developed to completely circumvent the judicial process. For example, the Modria online dispute resolution tool, developed from the eBay dispute resolution system, has been used to settle many thousands of disputes online using an AI system. The U.K. government is developing an Internet-based dispute resolution system that will be used to resolve minor (<£25,000) civil legal claims without any court involvement. Microsoft and the U.S. Legal Services Corporation have teamed up to provide machine learning legal portals to provide free legal advice on civil law matters to people who cannot afford to hire lawyers.

The Future of AI and the Law

These initial applications of AI to legal practice are just the early beginnings of what will be a radical technology-based disruption to the practice of law. AI "represents both the biggest opportunity and potentially the greatest threat to the legal profession since its formation."[14] The transformative impacts of AI on legal practice will continue to accelerate going forward. AI will take over a steadily increasing share of law firm billable hours, be applied to an ever-expanding set of legal tasks, and require knowledge and abilities outside the existing skill set of most current practicing attorneys. Today AI represents an opportunity for a law firm or an attorney to be a leader in efficiency, cost-effectiveness, and productivity, but soon incorporation of AI into practice will be a matter of keeping up rather than being a leader.

AI in the practice of law raises many broader issues that can only be briefly listed here. How will AI change law firm billing, where a smart AI system can conduct searches and analyses in a few seconds that formerly would have taken several weeks of an associate's billable time? If AI eliminates many of the more routine tasks in legal practice that are traditionally performed by young associates, how will this affect hiring and advancement of young attorneys? How will legal training and law schools need to change to address the new realities of AI-driven legal practice? How will AI affect the competitive advantage of large law firms versus small and medium-sized firms? Will companies start obtaining legal services directly from legal technology vendors, skipping law firms altogether? Will AI systems be vulnerable to charges of unauthorized practice of law? Given that AI systems increasingly use their own self-learning rather than preprogrammed instructions to make decisions, how can we ensure the accuracy, legality, and fairness of AI decisions? Will lawyers be responsible for negligence for relying on AI systems that make mistakes? Will lawyers be liable for malpractice for not using AI that exceeds human capabilities in certain tasks? Will self-learning AI systems need to be deposed and take the stand as witnesses to explain their own independent decision making?

One thing is certain—there will be winners and losers among lawyers who do and do not uptake AI, respectively. As one senior lawyer recently remarked, "Unless private practice lawyers start to engage with new technology, they are not going to be relevant even to their clients."[15] The AI train is leaving the station—it is time to jump on board. ◆

Endnotes

[1] Dana Remus & Frank S. Levy, Can Robots Be Lawyers? Computers, Lawyers, and the Practice of Law 46 (Nov. 27, 2016) (unpublished manuscript), https://ssrn.com/abstract=2701092.

[2] David Johnson, *Find Out If a Robot Will Take Your Job*, Time (Apr. 19, 2017), http://time.com/4742543/robots-jobs-machines-work/.

[3] *Deloitte Insight: Over 100,000 Legal Roles to Be Automated*, Legal IT Insider (Mar. 16, 2016), https://www.legaltechnology.com/latest-news/deloitte-insight-100000-legal-roles-to-be-automated/.

[4] Hugh Son, *JPMorgan Software Does in Seconds What Took Lawyers 360,000 Hours*, Bloomberg (Feb. 27, 2017), https://www.bloomberg.com/news/articles/2017-02-28/jpmorgan-marshals-an-army-of-developers-to-automate-high-finance.

[5] Bill Gates, The Road Ahead (1995).

[6] Joanna Goodman, Robots in Law: How Artificial Intelligence Is Transforming Legal Services 3 (2016).

[7] Julie Sobowale, *Beyond Imagination: How Artificial Intelligence Is Transforming the Legal Profession*, A.B.A. J., Apr. 2016, at 46, 48.

[8] Nick Bostrom, Superintelligence: Paths, Dangers, Strategies (2014).

[9] Thomas S. Clay & Eric A. Seeger, Altman Weil Inc., 2017: Law Firms in Transition 84 (2017), http://www.altmanweil.com/LFiT2017/.

[10] Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review*, 17 Rich. J.L. & Tech. 11, 43 (2011).

[11] Daniel Martin Katz et al., *A General Approach for Predicting the Behavior of the Supreme Court of the United States*, 12 PLoS ONE, 2017, https://doi.org/10.1371/journal.pone.0174698.

[12] Goodman, *supra* note 6, at 31.

[13] *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

[14] Goodman, *supra* note 6, at 129 (quoting Rohit Talwar).

[15] LexisNexis, Lawyers and Robots? Conversations around the Future of the Legal Industry 3 (2017) (comment of David Halliwell of U.K. law firm Pinsent Masons).

ARTICLE

Can Robots Be Lawyers?
Computers, Lawyers, and the Practice of Law

Dana Remus* & Frank Levy†

Abstract

We assess frequently advanced arguments that automation will soon replace much of the work currently performed by lawyers. In doing so, we address three weaknesses in the existing literature: (i) an insufficient understanding of current and emerging legal technologies; (ii) an absence of data on how lawyers divide their time among tasks; and (iii) inadequate attention to whether computerized approaches to a task conform to the values, ideals, and challenges of the legal profession. Combining a detailed technical analysis with a unique data set on time allocation in large law firms, we estimate that automation has a measurable impact on the demand for lawyers' time, but one that is less significant than popular accounts suggest. We then look ahead to future developments through a series of three questions. First, what is the likely path of technical innovation and diffusion in an unregulated market? Second, what are the benefits and adverse consequences of such a path? Third, to what extent can regulation reduce the adverse consequences of new technologies without reducing their benefits? Throughout the discussion, we ask how computers are changing—not simply replacing—the work of lawyers.

[*] Professor of Law, University of North Carolina School of Law. © 2017, Dana Remus & Frank Levy.

[†] Professor Emeritus, Department of Urban Studies and Planning, Massachusetts Institute of Technology and Research Associate, Department of Health Care Policy, Harvard Medical School.

The authors would like to thank: Jeanne Anderson; Andrew Arruda; David Autor; Kate Bartlett; Regina Barzilay; Joseph Blocher; Bernie Burke; Jill Burstein; David Curle; Randy Davis; Stuart Elliott; Bruce Elvin; Kathleen Engel; Bill Freeman; Ron Friedmann; Ken Grady; Maura Grossman; Dan Gutfreund; Eddie Hartman; Nathalie Hofman; Dan Jackson; Jim Jones; Jonathan Kash; Boris Katz; Scott Krowitz; Ruddick Lawrence; Nick Lemann; Maggie Lemos; Matt Levitt; Alex Levy; Marin Levy; Ryan McClead; Matthew McCubbins; Kyla Moran; Jean O'Grady; Steve Obenski; Ross Pascal; Christina Patterson; Joe Propcopio; Bob Rowe; Dan Rubins; Craig Smith; Jim Spohrer; Robin Toone; Doug Ventola; Jim Wagner; Noah Waisberg; Heathcoate Wales; Vern R. Walker; Ed Walters; Jessica Watts; Brad Wendel; Keith Winstein; Yuan Zhang; Pat Ziegler; and all participants of the 2015 Stanford Legal Ethics Schmooze, the William & Mary Faculty Law School Workshop, the Wake Forest Law School Faculty Workshop, and the MIT CSAIL/Economics lunch series and the MIT Sloan School IWER Seminar. We are particularly grateful to Consilio's Sky Analytics for their generous provision of data and to the Spencer Foundation for supporting Frank Levy's work.

TABLE OF CONTENTS

INTRODUCTION

On March 14, 2011, a *New York Times* headline read: "Armies of Expensive Lawyers, Replaced by Cheaper Software."[1] In the article, *Times* technology reporter John Markoff described how computers, capable of identifying relevant words and phrases, were displacing large numbers of lawyers in discovery practice. The article posed a warning to lawyers as well as to other professionals: computers could replace humans in a highly educated, white-collar occupation.

The warning has become common wisdom. Scholars, lawyers, and commentators alike are now predicting the end of the legal profession, citing specific examples of computers successfully performing lawyers' jobs.[2] Predictive

[1] John Markoff, *Armies of Expensive Lawyers, Replaced by Cheaper Software*, N.Y. TIMES, Mar. 4, 2011, at A1.

[2] Richard and Daniel Susskind argue that lawyers, among other professionals, face a future in which "increasingly capable machines, autonomously or with non-specialist users, will take on many of the tasks that currently are the realm of the professions." RICHARD SUSSKIND & DANIEL SUSSKIND, THE FUTURE OF THE PROFESSIONS: HOW TECHNOLOGY WILL TRANSFORM THE WORK OF HUMAN EXPERTS 231 (2015); *see also* RICHARD SUSSKIND, TOMORROW'S LAWYERS: AN INTRODUCTION TO YOUR FUTURE (2013); RICHARD SUSSKIND, THE END OF LAWYERS: RETHINKING THE NATURE OF LEGAL SERVICES (2010). Law professors John McGinnis and Russ Pearce contend that "the disruptive effect of machine intelligence will trigger the end of lawyers' monopoly." John O.

coding, the subject of Markoff's article, is a machine learning application that automates document classification in discovery practice.[3] Ross Intelligence, a legal application of IBM's Watson, advertises the ability to provide concise answers to natural language legal questions.[4] LegalZoom, RocketLawyer, and other online legal service providers produce basic wills, divorce agreements, contracts, and incorporation papers without a lawyer's involvement.[5] These technologies challenge the traditionalist view that lawyering is irreducibly human, and force us to recognize that computers are changing the way law is practiced.

From one perspective, the dramatic impact of technology on legal practice is nothing new. The Internet, email, and legal research databases like Westlaw and Lexis have been impacting and altering legal practice for decades.[6] But from another perspective, we may be on the precipice of a more fundamental shift.

McGinnis & Russell G. Pearce, *The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services*, 82 Fordham L. Rev. 3065 (2014). Other commentators predict that "[i]n the not-too-distant future, artificial intelligence systems will have the ability to reduce answering a legal question to the simplicity of performing a search," Josh Blackman, *The Path of Big Data and the Law* 1 (S. Tex. Coll. of Law Houston Working Paper Grp., 2013). Furthermore, scholars have stated, "[o]nce we have fully artificial intelligence enhanced programs like LegalZoom, there will be no need for lawyers, aside from the highly specialized and expensive large-law-firm variety." Paul Lippe & Daniel Martin Katz, *10 Predictions About How IBM's Watson Will Impact the Legal Profession*, A.B.A. J. (Oct. 2, 2015), http://www.abajournal.com/legalrebels/article/10_predictions_about_how_ibms_watson_will_impact/ [https://perma.cc/UHY4-TPLK]; *Professor Dr Robot QC*, Economist (Oct. 15, 2015), http://www.economist.com/news/business/21674779-once-regarded-safe-havens-professions-are-now-eye-storm-professor-dr-robot [https://perma.cc/YN7A-8578]; Debra Cassens Weiss, *Will Newbie Associates be Replaced by Watson?*, A.B.A. J. (Oct. 26, 2015), http://www.abajournal.com/news/article/will_associates_be_replaced_by_watson_computing_35_percent_of_law_firm_lead/?utm_source=maestro&utm_medium=email&utm_campaign=tech_monthly [https://perma.cc/NHU9-LX3A] [hereinafter Weiss, *Newbie Associates*]; *see also* Martin Ford, Rise of the Robots: Technology and the Threat of a Jobless Future (2015); Jerry Kaplan, Humans Need Not Apply: A Guide to Wealth and Work in the Age of Artificial Intelligence (2015).

[3] *See* Markoff, *supra* note 1.

[4] *See, e.g.*, Weiss, *Newbie Associates*, *supra* note 2. Ross Intelligence is developing one such application, which it describes as your "brand new Super Intelligent Attorney." *See* Ross Intelligence, http://www.rossintelligence.com/ [https://perma.cc/DN24-DV4M] (last visited Apr. 3, 2017) ("You ask your questions in plain English, as you would a colleague, and ROSS then reads through the entire body of law and returns a cited answer and topical readings from legislation, case law and secondary sources to get you up-to-speed quickly.").

[5] *See, e.g.*, Benjamin Barton, Glass Half Full: The Decline and Rebirth of the Legal Profession (2015) [hereinafter Barton, Glass Half Full]; Benjamin Barton, *The Lawyer's Monopoly: What Goes and What Stays*, 82 Fordham L. Rev. 3068 (2014) [hereinafter Barton, *The Lawyer's Monopoly*]; Benjamin Barton, *Lessons from the Rise of LegalZoom*, Bloomberg BNA, at A1 (June 18, 2015), https://bol.bna.com/lessons-from-the-rise-of-legalzoom/ [https://perma.cc/F9UV-LSY3].

[6] Debra Cassens Weiss, *Will Technology Create a Lawyer 'Jobs-pocalypse'?*, A.B.A. J. (Jan. 5, 2016), http://www.abajournal.com/news/article/does_technology_presage_a_lawyer_jobs_pocalypse_naysayers_overstate_impact/ [https://perma.cc/22R3-HRK8] ("Word processing revolutionized document drafting. The Internet permitted rapid document transmission and video conferencing; accelerated the breakdown of law firms' information monopoly on rates, services, and clients; and increased clients' ability to spread legal work among multiple law firms. Email increased the speed and ease of communication both among lawyers and between lawyers and clients, and expanded the number of associates a single partner could supervise and so has facilitated the growth of large law firms.").

Machine learning applications appear poised to displace lawyers, to make inroads on the profession's monopoly, and to open new ways of addressing the access to justice gap.

In this Article, we examine prevalent claims and predictions surrounding new legal technologies, including that they are triggering the imminent and widespread displacement of lawyers by computers. In doing so, we seek to add depth and nuance to the conversation in three ways. First, we engage with technical details. We appreciate why much existing work does not—specifics blur the headlines and may be uninteresting to lay readers. But the details are critical for understanding the kinds of lawyering tasks that computers can and cannot perform. The details explain, for example, why document review in discovery practice is more amenable to automation than in corporate due diligence work, and why the automation of Associated Press sports stories and short memos on questions of law do not suggest the imminent automation of legal brief-writing.[7] The details also offer useful insights on what is likely to be automated in the foreseeable future. We therefore offer a detailed review of salient legal technologies based on a set of unstructured interviews over an eighteen-month period with computer scientists, legal technology developers, and practicing lawyers. Second, we ground our analysis in lawyer time usage data provided by Sky Analytics, a division of Consilio.com.[8] Lacking such data, existing employment predictions remain mere speculation. For example, scholars suggest that the automation of document review is displacing large numbers of junior associates without reference to the amount of time junior associates previously spent on document review.[9] Our data cast doubt on these predictions.

Third, we grapple with the intersection of technological advances, access to justice, and professionalism. Many scholars maintain that "professionalism" is a mere cover for lawyer protectionism, and that the public interest is best served by commoditizing and computerizing as many legal services as possible.[10] Doing

[7] *See infra* notes 67–68 and accompanying text.

[8] Sky Analytics assists corporate clients in monitoring and analyzing the clients' legal expenditures. *See Sky Analytics*, CONSILIO, http://www.consilio.com/technology/sky-analytics/ [https://perma.cc/6L9K-TMWD] (last visited Apr. 3, 2017). The data suffers from a number of limitations, discussed below, but is nevertheless useful in providing a general picture of how lawyers spend and bill their time.

[9] *See, e.g.*, McGinnis & Pearce, *supra* note 2, at 3047–48.

[10] Critics have long maintained that the professional form inures to the benefit of lawyers themselves at the expense of society by facilitating protectionism. *See, e.g.*, SUSSKIND & SUSSKIND, *supra* note 2, at ch. 1; RICHARD L. ABEL, AMERICAN LAWYERS 20 (1989); ANDREW ABBOTT, THE SYSTEM OF PROFESSIONS: AN ESSAY ON THE DIVISION OF EXPERT LABOR 184–86 (1988); JEROLD S. AUERBACH, UNEQUAL JUSTICE: LAWYERS AND SOCIAL CHANGE IN MODERN AMERICA 88, 92, 99–102 (1976); MAGALI SARFATTI LARSON, THE RISE OF PROFESSIONALISM: A SOCIOLOGICAL ANALYSIS xvii (1977). Certainly, individual lawyers and the organized bar have at times acted in protectionist and self-serving ways. But to conclude that the professional form is therefore undesirable is to ignore the many ways in which the profession is constitutive of the state and critical to the rule of law. *See* Robert W. Gordon & William H. Simon, *The Redemption of Professionalism?*, *in* LAWYERS' IDEALS/LAWYERS' PRACTICES: TRANSFORMATIONS IN THE AMERICAN LEGAL PROFESSION 235 (Robert L. Nelson et al. eds., 1992); *see*

so, they contend, will lower costs and increase access.[11] Unquestionably, the profession acts in self-interested and troubling ways at times; undoubtedly, new technologies are opening promising paths for addressing the access to justice gap. But we believe that the requisite analysis is much more complex than existing accounts acknowledge.

Our discussion proceeds in two parts. In Part I, we address the extent of computer displacement of lawyer labor, seeking a more nuanced understanding than is offered in the existing literature. We use data from Consilio's Sky Analytics to test two pieces of conventional wisdom—that the overall employment impacts of computers on lawyers are significant, and that the effects are the greatest among junior associates. After reviewing near-term capabilities of computers to automate various categories of lawyering tasks, we argue that there is no strong relationship between computers' employment effects and positions within a firm. Even where automation has made significant progress, its impact has been less than the headlines would have us believe.[12]

In Part II, we explore the longer-term evolution of legal technologies by reference to three core lines of inquiry. First, we ask how legal technologies would likely develop in an unregulated market. Next, we consider the approach of existing regulatory structures, and argue that such structures unnecessarily impede the development and adoption of new technologies. Finally, we argue for the ongoing value of professional norms and regulation, notwithstanding significant problems with existing approaches. The challenge, we conclude, is to design regulatory structures that protect professional values without impeding the advance of new legal technologies.

Throughout this discussion, we focus on the ways in which computers are changing—not simply replacing—the work of lawyers. We argue that the relevant evaluative and normative inquiries must begin with an understanding of how computers perform various lawyering tasks differently than humans, and the ways in which those differences impact not only individual clients, but also the legal system writ large.

also Dana A. Remus, *Reconstructing Professionalism* (Apr. 30, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676094 [https://perma.cc/J359-LT4B] [hereinafter Remus, *Reconstructing Professionalism*].

[11] *See, e.g.*, McGinnis & Pearce, *supra* note 2, at 3054–55; James E. Cabral et al., *Using Technology to Enhance Access to Justice*, 26 HARV. J.L. & TECH. 241, 246–56 (2012); William E. Hornsby, Jr., *Gaming the System: Approaching 100% Access to Legal Services Through Online Games*, 88 CHI.-KENT L. REV. 917, 931–34 (2013); Ronald W. Staudt, *All the Wild Possibilities: Technology that Attacks Barriers to Access to Justice*, 42 LOY. L.A. L. REV. 1117, 1128–34 (2009); Michael J. Wolf, *Collaborative Technology Improves Access to Justice*, 15 N.Y.U. J. LEGIS. & PUB. POL'Y 759, 773–85 (2012).

[12] As we explain below, the loss of junior associate jobs has been occurring over time. It is likely driven by significant weakness in the market for lawyers that accelerated with the 2008 financial collapse. By that time, much of "traditional" junior associate work—for example, document review in discovery—had already been farmed out to contract lawyers. *See infra* Part I.

I. EMPLOYMENT EFFECTS

In this Part, we first present data on how much lawyer time is devoted to various categories of lawyering work. We then review a set of basic ideas in artificial intelligence and use the ideas to explain computers' varying capacities to automate these work categories. Finally, we translate the extent of automation into a rough picture of how much lawyer time is being displaced by computers.

We anchor the discussion in the current and foreseeable trajectory of these technologies in the present and mid-term future (roughly the next decade). The resulting analysis is admittedly linear, risking that we underestimate the likelihood and impact of radical future innovation. But those who predict radical innovation have some responsibility to explain their reasoning. Simply invoking Moore's Law or pointing to an undefined future[13] creates an argument that defies proof or refutation, and that therefore fails to inform the debate in a meaningful way.

A. THE DATA

Our data on time usage comes from Consilio's Sky Analytics of Framingham, Massachusetts,[14] a consulting firm that provides corporate clients with aggregation and analysis of invoices billed by law firms. Typically, each invoice covers a small increment of time and describes the work the lawyer performed by reference to a task code from the ABA's Uniform Task-Based Management System (UTBMS).[15] The UTBMS consists of 114 distinct task codes, which we have aggregated into thirteen categories for purposes of identifying patterns.[16] Sky Analytics supplements the invoice with information on the submitting lawyer, including their status within the firm (associate or partner) and how many years they have been practicing.

For purposes of this project, Sky Analytics provided us with a blinded data set of invoices for 2012 through early 2015 that allowed us to construct the following information[17]:

[13] For example, Susskind and Susskind argue the post-professional society will be reached "in the fully fledged, technology-based Internet society." SUSSKIND & SUSSKIND, *supra* note 2, at 232.

[14] *Sky Analytics*, *supra* note 8.

[15] *See Uniform Task-Based Management System*, AM. BAR ASS'N SECTION OF LITIG., http://www.americanbar.org/groups/litigation/resources/uniform_task_based_management_system.html [https://perma.cc/FS3P-7RCM] (last visited Apr. 3, 2017) (a set of billing codes designed to standardize the categorization of tasks).

[16] Our thirteen aggregated tasks are: Advising Clients; Other Communications/Interactions; Case Administration and Management; Court Appearances; Document Drafting; Document Management; Document Review; Due Diligence; Fact Investigation; Legal Analysis and Strategy; Legal Research; Legal Writing; and Negotiation.

[17] Because Sky Analytics' customer base changed from year to year, the multiple years of data were not suitable for examining trends.

- Distribution of hours billed by task.
- Distribution of hours billed by task further disaggregated by law firm size in five "Tiers" (Tier 1 > 1000 lawyers through Tier 5 < 25 lawyers).
- Distribution of hours billed by task and law firm size, further disaggregated by position in the firm (Associate ≤ 2 years; Associate > 2 years; Partner).

These data have a number of limitations. First, the original UTBMS codes (and hence our thirteen aggregated codes) allow lawyers significant discretion in how they record their time, painting at best a rough picture of time usage.[18] Second, the data provide no information on the work patterns of solo practitioners, who comprise about forty percent of all practicing lawyers,[19] or contract attorneys, whether hired by the law firm or the client.[20] It therefore focuses our analysis on law firm lawyers, primarily in the corporate hemisphere. Finally, because the invoices come from corporate clients, SkyAnalytics cannot provide a complete set of invoices billed by a single or several law firms.

Nevertheless, the data set is quite large—2014 invoices alone totaled $2.31B—and we (and Sky Analytics) believe that a pooled sample of all billing from firms with 1000 or more lawyers (Tier 1 firms) provides a rough approximation of the distribution of hours billed to each task by junior associates (two years or less), senior associates, and partners in a typical large law firm.[21] The data suggest that time-on-task among smaller sample firms (Tiers 2 through 5) follow a similar distribution.

Specifically, Table 1 lists the thirteen aggregated task codes with two distributions of hours spent on task: the 2012–2015 distribution of time-on-task billed by all Tier 1 firms (> 1000 lawyers) and the 2012–2015 distribution of time-on-task for all Tier 2–5 firms (all other firms in the Sky Analytics sample). We list the tasks in order of difficulty to automate—what we describe as machine complexity—which we analyze below.

[18] Errors can entail both mislabeled time and inaccurately recorded amounts of time. Billing partners may also revise time allocations prior to sending an invoice to the client. For example, one interviewee explained that clients do not like to see large amounts of time invoiced to legal research, so billing lawyers might reallocate that time to the task the research is associated with, the broad category of "legal analysis and strategy," or a category of unbilled time. Telephone Interview with Jean P. O'Grady, Author of the Dewey B Strategic Blog & Senior Dir. of Research Servs. at an Am Law 100 law firm (July 22, 2015).

[19] CLARA N. CARSON & JEEYOON PARK, THE LAWYER STATISTICAL REPORT: THE U.S. LEGAL PROFESSION IN 2005, at 6 (2012).

[20] Nor does the data account for time billed to business development or other internal matters not billed to clients.

[21] The distribution of hours billed is not precisely the same as the distribution of tasks in the firm because firms bill less than 100% of junior associates' hours.

TABLE 1
PERCENT OF INVOICED HOURS SPENT ON VARIOUS TASKS—2012–2015

Task	Tier One Firms	Tier Two–Five Firms
Document Management	0.4%	0.7%
Case Administration and Management	3.7%	5.6%
Document Review	4.1%	3.6%
Due Diligence	2.0%	3.4%
Document Drafting	5.0%	4.0%
Legal Writing	11.4%	17.7%
Legal Research	0.5%	0.4%
Legal Analysis and Strategy	28.5%	27.0%
Fact Investigation	9.2%	9.6%
Advising Clients	9.3%	3.2%
Negotiation	3.0%	5.0%
Other Communications/Interactions	8.8%	5.0%
Court Appearances and Preparation	13.9%	14.5%
Totals**	99.8%	99.7%

** Percentages may not sum to 100% due to rounding.

B. AUTOMATING LEGAL WORK

Translating Table 1 into employment effects requires an analysis of each category of legal work to understand the current and near-term potential for automation. In preparation for that analysis, we review here a set of basic ideas from artificial intelligence that undergird all legal software.

1. MODELING INTELLIGENCE

We begin with two observations: (i) virtually all of a lawyer's tasks[22] involve the processing of information[23] and (ii) a computer processes information by executing instructions. It follows that for a computer to automate a lawyer's task, it must be possible to model the lawyer's information processing in a set of

[22] We follow the economists' convention of describing a job as a collection of tasks because many computer applications automate a part of a job rather than the whole job. *See* David H. Autor et al., *The Skill Content of Recent Technological Change: An Empirical Exploration*, 118 Q.J. ECON. 1279, 1279–1333 (2003).

[23] For example, a lawyer processes information about family relationships and assets into a will, or transaction information into a contract. Information processing, which we define broadly as changes in the form, organization, storage, or use of information, is central to virtually all human work.

instructions. In other words, computers can automate those lawyer's tasks that are "structured" or "routine."

The tasks are modeled using both *deductive instructions* and *data-driven instructions*. Deductive instructions model information processing where the structure is readily apparent—searching a legal database for opinions from a particular judge or court, or populating fields in a legal form with relevant names or other information.[24]

Data-driven instructions arise where the structure of information processing is not apparent—the way in which an individual makes a decision as to what she will eat for lunch. In some cases, it is possible to approximate this information processing by estimating a statistical model that relates the information output to the information inputs, treating the intervening steps as a black box. Data-driven instructions are the estimated equations of such a statistical model.

Consider the problem of predicting how a judge might rule in a legal malpractice case. The information *inputs* include the facts of the case and the elements of the cause of action; the information *output* is the judge's decision. The relationships between inputs and output are often complex and opaque, but can nevertheless be approximated by a statistical model based on a set of the judge's prior decisions in similar cases. The model can be sketched as follows:

Equation 1: $Y_i = \beta_1 X_{1i} + \beta_2 X_{2i} \ldots\ldots\ldots + \mu_i$

Where: $Y_i = 1$ if the judge decides in favor of the plaintiff in the i'th case;

$= 0$ if the judge decides in favor of the defendant in the i'th case;

$X_{1i}, X_{2i} \ldots.$ are case characteristics drawn from the record of the i'th case;

$\beta_1, \beta_2 \ldots.$ are the estimated coefficients of the case characteristics, including the facts of the case and elements of the cause of action; and

μ_i is a stochastic error term for the i'th judicial decision.

This estimation process is called "training" or "supervised (machine) learning"—supervised because the estimation requires the parameters to align with the judge's prior decisions; learning because the estimation process can be seen as learning the relationship (summarized in β's) between the case characteristics and the judge's decisions.[25] Once estimated, Equation 1 becomes a data-driven instruction—an instruction that can be applied to characteristics of a new case to predict judge's decision.

[24] In the early days of artificial intelligence, it was assumed most tasks could be described in deductive instructions (also called rules-based logic), but this proved incorrect.

[25] The estimation process is also described as training or as a form of pattern recognition, as the computer searches for the pattern of application information that best predicts a default.

Data-driven instructions also can arise from "unsupervised (machine) learning," which encompasses techniques to uncover patterns in a data set that can form the basis for subsequent analysis. Latent semantic analysis (LSA), an example of unsupervised learning, plays multiple roles in legal software.[26] For example, it creates a basis for determining whether two pieces of text are close in meaning—a measure that is useful in automating whether a particular passage is responsive to a question, or whether clauses in two contracts are conceptually similar. Testing for similar meaning involves more than asking whether the same words appear in two texts because different words can be used to convey the same meaning—for example, "automobile" and "vehicle." Conversely, two documents can refer to different topics even while using the same word—computer chip, paint chip, chocolate chip.

LSA exploits the insight that a word's meaning in a piece of text is partially established by its context. Beginning with a set of documents (or a number of pieces of text), the analysis first constructs a term-document matrix (Figure 1), in which each cell contains the number of times a particular term or word[27] appears in a particular document. Using unsupervised learning, LSA software uses correlations among words in a document to identify "word clusters"—words that usually appear in the same document when they appear in the set of documents.

FIGURE 1
TERM-DOCUMENT MATRIX

	Document #1	**Document #2**	**Document #3, etc.**
Term #1	T_{11}	T_{12}	T_{13}
Term #2	T_{21}	T_{22}	T_{23}
Term #3	Etc.		
Term #4			

Consider a set of 1000 documents. Suppose that the term "automobile" appears in 100 of these documents, 90 of which also include the words "safety," "braking," and "distance." If the words "safety," "braking," "distance," and "vehicle" (but not "automobile"), appear in another 120 documents in the set, the chances are reasonable that (a) "automobile" and "vehicle" represent the same concept in these documents and that (b) the two sets of documents involving "safety," "braking," and "distance" are invoking similar meanings. LSA identi-

[26] In recent years, much of what LSA does is also being accomplished through probabilistic language models that use neural nets (i.e., "deep learning"). *See Vector Representations of Words*, TENSORFLOW, https://www.tensorflow.org/versions/r0.11/tutorials/word2vec/index.html [https://perma.cc/KH96-WYVZ] (last updated Dec. 20, 2016). We focus on LSA here because the logic is more intuitive.

[27] "Words" in this description exclude "the," "and," "this," and similar words that typically appear in every piece of text. In natural language processing, these words are called "stop words."

fies all clusters in the set of documents and then mathematically represents each document in terms of the clusters it contains. A pair of documents, represented in this way, can then be measured for their similarity of meaning.[28]

Machine learning models—both supervised and unsupervised—offer useful perspective on the argument that the work of lawyers (and other professionals) is more routine than we recognize.[29] Return to the modeling of a judge's decision—if the model fits the data, it is equivalent to saying that the judge reaches his decisions through a tacit mental protocol that ensures the same result for all cases with the same characteristics. Stated otherwise, the judge's decision-making process is "structured" or routine. Because the mental protocol is tacit—and not easily articulated—the judge may not experience his decisions as routine, but the machine learning model makes the tacit protocol explicit as a mathematical combination of characteristics taken from the case (Equation 1), which can then be used to predict future judicial decisions. In this way, machine learning unravels a part of Michael Polyani's paradox that "[w]e know more than we can tell."[30]

There are, however, limits to machine learning's ability to reveal and formalize routine work. Most importantly, the task being modeled must have underlying, if unrecognized, structure—it must *actually* be routine. If, over time, the judge makes different decisions when faced with the same case characteristics, then the model will not fit the data[31] and it will have limited predictive power (as befits an unpredictable judge).

In addition, the model's predictive ability is restricted to cases that are generally similar to the judge's past cases on which the model was estimated. If the past cases all involved female plaintiffs, the model may not correctly predict the judge's decision in cases with a male plaintiff. More generally, machine learning models—estimated statistical models—have difficulty processing contingencies that lie outside the data on which they were trained. Thus, just as computer-based question-answering systems have problems confronting questions that differ sharply from the questions on which they were trained, autonomous vehicles have problems navigating road hazards not included in their training data, and so on.[32] We return to this point below.

[28] The basic LSA reference is Scott Deerwester et al., *Indexing by Latent Semantic Analysis*, 41 J. AM. SOC'Y FOR INFO. SCIENCE 391, 391–407 (1990). The representation of documents in terms of clusters is roughly equivalent to principal components analysis.

[29] *See* SUSSKIND & SUSSKIND, *supra* note 2.

[30] MICHAEL POLANYI, THE TACIT DIMENSION 4 (1966).

[31] In a well-estimated model, the coefficients (the β's) should be statistically significant and the equation as a whole should have a reasonably high squared correlation coefficient (R2).

[32] Google, Uber, Ford Motor Company, and others are currently engaged in large-scale data collection efforts for autonomous vehicles, with particular emphasis on collecting rare but dangerous events. *See, e.g.*, Johana Bhuian, *Uber's Autonomous Cars Drove 20,354 Miles and Had to Be Taken Over at Every Mile, According to Documents*, RECODE (Mar. 16, 2017), https://www.recode.net/2017/3/16/14938116/uber-travis-kalanick-self-driving-internal-metrics-slow-progress [https://perma.cc/CMT9-T5E9].

There are, finally, a significant number of legal tasks that are too complex to be modeled by any set of instructions (at least at the present time). Unscripted human interaction falls into this category because it often depends on formulating responses to unanticipated questions and statements. This, in turn, requires recognizing the broader context in which words are being used—not only the surrounding words (as in LSA), but the identity and motivation of the speaker and the purpose of the communication.

Understanding context frequently requires recognizing the affect of the person making the statement. Certainly, progress has been made in the field of "affective computing,"[33] enabling computers to recognize a user's affect by measuring physiological states and facial expressions.[34] But as a leader of the field explains, it is one thing to differentiate between "user is frustrated" and "user is not frustrated," or even to differentiate between basic emotional states such as anger, fear, sadness, and love.[35] It is quite another, and much more difficult, for a computer to recognize and label the infinite array of more complex emotional states that we ourselves can rarely label, but that we nevertheless navigate using the tacit skills of emotional intelligence.[36] Such tasks lack sufficient structure to be modeled as a set of deductive or data-driven instructions and cannot be automated at this time.

2. SPECIFIC APPLICATIONS

With this background in mind, we turn to a more specific discussion of the current and likely automation of the categories of legal work. After describing the extent of automation, we label each category as subject to light, moderate, or heavy employment effects. These are, by necessity, "eyeball" classifications but they rest on examination of current and near-term technology. For example, predictive coding software clearly has a "heavy" effect on employment in document classification. In contrast, contract review software automates the search for problematic obligations in a potential acquisition, but this is only a part of the due diligence process and we classify this software as having a moderate employment effect. By adopting a partial equilibrium approach—assuming that the demand for legal work is constant so that the automation of any task results in reduced employment—we focus narrowly on automation's current impact (while

[33] *See* ROSALIND W. PICARD, AFFECTIVE COMPUTING (2000).

[34] Juan Martinez-Miranda & Arantza Aldea, *Emotions in Human and Artificial Intelligence*, 21 COMPUTERS IN HUM. BEHAV. 323 (2005); *Special Issue on Affective Computing*, 59 INT'L J. HUM.-COMPUTER STUD. 1 (2003); *see* Aditya Khosla et al., *Modifying the Memorability of Face Photographs* (2013), http://people.csail.mit.edu/khosla/papers/iccv2013_khosla.pdf [https://perma.cc/PHG4-ZQ6D] (paper presented at the International Conference on Computer Vision (ICCV)).

[35] Rosalind W. Picard, *Affective Computing: Challenges*, 59 INT'L J. HUM.-COMPUTER STUD. 55, 58 (2003).

[36] *See* Xiaobai Li et al., *Reading Hidden Emotions: Spontaneous Micro-expression Spotting and Recognition*, CORNELL UNIV. LIBR. (Nov. 2, 2015), http://arxiv.org/abs/1511.00423v1 [https://perma.cc/6HV2-V6HR].

recognizing that automation is only one among several factors shaping the market for legal services[37]). In the long run, this is an unrealistic assumption,[38] but in recent years, it has proven plausible.[39] Moreover, it offers a transparent basis on which to begin to estimate automation's effects.

3. DOCUMENT MANAGEMENT (LIGHT EMPLOYMENT IMPACT)

The first category in Table 1, document management, entails applications designed to increase workflow efficiency, including by creating, populating, and maintaining databases and filing systems. Some aspects of this work have long been automated by networked computers and servers, and by software that can sort and search files. For decades, large firms have been using document management software that centralizes, stores, and organizes all of a firm's files, allowing all lawyers within the firm to search for and retrieve particular documents. More recent products have expanded to include automated templating, entry and billing of lawyers' hours, and the tracking of trust accounts.[40] With a few exceptions—most notably, optical character recognition to process scanned documents—these products are built using deductive instructions. We refer to them as productivity applications.

For two reasons, we believe document management productivity applications will have only a light impact on lawyer employment. First, many of these products have existed for years such that any impact would have taken effect long ago. Second, many of these tasks were previously performed by paralegals or

[37] Consider, for example, that the introduction of Automatic Teller Machines (ATM) was expected to reduce the number of teller jobs per 1000 population by lowering the number of tellers per branch bank. In practice, fewer tellers per branch bank meant branch banks were cheaper to operate and for a time, the number of teller jobs per 1000 population increased, because many bank corporations began to compete by opening large numbers of branches.

[38] By many estimates, more than seventy-five percent of civil legal need in the country goes unmet. *See* Deborah L. Rhode, *Whatever Happened to Access to Justice?*, 42 LOY. L.A. L. REV. 869, 869–70 (2009). The automation of lawyering tasks may address this latent market rather than replacing existing lawyer labor. Alternatively, it may push lawyers to serve this latent market as a means of finding new work.

[39] See CTR. FOR THE STUDY OF THE LEGAL PROFESSION, GEORGETOWN UNIV. LAW CTR. & THOMSON REUTERS PEER MONITOR, 2016 REPORT ON THE STATE OF THE LEGAL MARKET 4, chart 3 (2016), https://peermonitor.thomsonreuters.com/wp-content/uploads/2016/01/2016_PM_GT_Final-Report.pdf [https://perma.cc/74DD-76WW] [hereinafter 2016 LEGAL MARKET REPORT], which shows very little growth in billings since 2010 for a sample of Am Law 100 and 200 firms. Similarly, data from the U.S. Department of Commerce "National Income and Product Accounts" on the value of legal services show that between 1990 and 2007, the value of legal services (adjusted for inflation) grew at an average rate of 12.8 percent. Between 2007 and 2013, the growth rate was −0.6 percent while the number of lawyers in the country continued to grow (by an annual 1.9 percent). U.S. Dep't of Commerce: Bureau of Economic Analysis, *Interactive Data,* tbls.6.1 B–C, http://www.bea.gov/iTable/iTable.cfm?ReqID=9&step=1#reqid=9&step=1&isuri=1 [https://perma.cc/UU2V-GTS7] (last visited Apr. 2, 2017).

[40] *See, e.g.*, LAWBASE, http://lawbase.com/ [https://perma.cc/4NUN-RF5P] (last visited Apr. 2, 2017); ROCKET MATTER, https://www.rocketmatter.com/legal-billing-software/ [https://perma.cc/4F5N-6S2Y] (last visited Apr. 2, 2017); MYCASE, www.mycase.com [https://perma.cc/D8ZZ-7ZBA] (last visited Apr. 2, 2017).

clerical staff, such that they, and not lawyers, would likely feel the impact of any continuing labor displacement.

4. CASE ADMINISTRATION AND MANAGEMENT (MODERATE IMPACT)

Case administration and management encompasses tasks such as budgeting, billing, assigning and monitoring workflow, retaining experts, and managing contracts. Some of these tasks, like those that comprise document management, have been successfully automated by the umbrella productivity applications just described, which primarily impact paralegals and legal assistants.[41] Some emerging products, however, use machine learning to perform aspects of contract management currently performed by lawyers. For example, KM Standards advertises software that reviews all of a company's contracts in a particular area, extracts the common provisions, and creates a basic template.[42] The software also highlights discrepancies between the template and contracts proposed by other parties. Both tasks involve identifying similar meaning between pieces of texts and are likely accomplished using LSA or a probabilistic language model.[43]

KM Standards joins other companies whose products, if frequently used, could have a meaningful impact on the demand for lawyers' work in the corporate sphere. Kira Systems offers software that pulls analogous provisions from different contracts into summary charts and compares particular provisions or entire documents, highlighting different contracting strategies.[44] Kira Systems' software also facilitates team and task management by organizing and monitoring task assignment and by keeping track of which documents and provisions have been reviewed and which have not. Software by the British company, Ravn, performs similar tasks and has also made strides in grouping documents by meaning, as well as in searching for particular pieces of information in an organization's files.[45]

Other aspects of case management, in contrast, lie well beyond the current capacity of computers. Tasks such as monitoring junior lawyers' work or dealing with parties who fail to honor contractual obligations require unstructured human interaction of a kind that computers cannot currently perform.[46] This will no doubt change, particularly as technologies like Kira Systems increasingly

[41] *See supra* note 40 and accompanying text.

[42] KM STANDARDS, http://kmstandards.com [https://perma.cc/Y46S-KVUB] (last visited Apr. 2, 2017).

[43] This is speculation on our part. As noted earlier, some processing previously done using LSA is now using probabilistic language models and neural networks.

[44] *See, e.g.*, KIRA, https://kirasystems.com/ [https://perma.cc/XP4F-XNZF] (last visited Mar. 2, 2017); CONTRACTASSISTANT, www.contractassistant.com [https://perma.cc/J9AX-9V2G] (last visited Apr. 2, 2017). These and other applications encompass such tasks as filing documents, identifying differences between successive drafts of contracts, and issuing alerts on due dates of contractual obligations.

[45] RAVN Systems, https://www.ravn.co.uk [https://perma.cc/L5JQ-35ET] (last visited Apr. 2, 2017).

[46] In theory, software could allocate a payment if a contract provision was breached, but this would require agreement that a breach had actually occurred.

facilitate task management. For now, however, we combine a potentially significant impact of automation on demand for lawyers in contract management with the unlikely impact in these other areas, and conclude that automation is having a moderate overall employment impact on the tasks of case management and administration.

5. DOCUMENT REVIEW (STRONG IMPACT)

The essence of document review—which we define as reviewing documents for purposes of discovery in litigation or government investigations—is the lawyer's judgment that the content of a given document is or is not responsive to an opposing party's requests for information. Lawyers have been automating aspects of this work since the 1990s, when the explosion of electronically stored information[47] demanded some means of culling through massive electronic data sets. Early attempts, which relied on deductive instructions to search documents for keywords or combinations of keywords[48] that suggested responsiveness,[49] were highly flawed. As noted in our discussion of LSA, particular meanings and content do not necessarily correlate with specific words. As a result, searching only for specific words produces results that are both under-inclusive (risking that important documents were being overlooked) and over-inclusive (raising the costs of review by returning large quantities of non-responsive documents).[50]

More recently, a number of vendors have begun marketing predictive coding technologies that use machine learning to model more accurately the basis of the human judgment regarding responsiveness. "Predictive coding" is an umbrella term encompassing significant variations and multiple products.[51] Under early versions, supervising lawyers[52] would review a "training sample" of documents (perhaps one or two thousand) from among the full data set (likely hundreds of thousands or millions of documents), classifying each document as responsive or not.[53] The software would then scan the training sample and estimate a supervised learning model similar in spirit to Equation 1, above. In this model, the outcome variable—"Y"—is a (0,1) variable describing the lawyers' classification of the document as "responsive" or "not responsive." The information inputs—"X's"—capture characteristics of the document such as frequency of

[47] Dana Remus, *The Uncertain Promise of Predictive Coding*, 99 IOWA L. REV. 1691, 1698 (2014) [hereinafter Remus, *Predictive Coding*].

[48] A typical keyword search rule involving the competitive behavior of a corporation might be: Select Document if: [Price] is within fifteen words of ["customer"] or ["competitor"]. The program would then return all documents meeting the search criteria.

[49] Remus, *Predictive Coding*, *supra* note 47, at 1698.

[50] *Id.*

[51] *Id.*

[52] Initially, the training sample was coded by partners or senior associates familiar with the case. Anecdotally, the task has already been pushed down to more junior lawyers.

[53] Remus, *Predictive Coding*, *supra* note 47, at 1702.

keywords, “n-grams” (three or four word sequences), word clusters derived from LSA, or other document characteristics.[54] The estimated model was then used to classify each of the remaining documents pursuant to an ex ante probability of relevancy.

Since 2012, when a federal judge first issued an opinion blessing predictive coding as an acceptable means of meeting discovery obligations,[55] use of the software has steadily increased and a number of variations have entered the market.[56] Pursuant to the most effective currently available protocol, called “continuous active learning,” supervising lawyers start by using keyword searching to select an initial set of potentially relevant documents, which they rank for relevancy.[57] These documents form the seed set and are then used to create a statistical model designed to predict responsiveness.[58]

Studies show that many predictive coding technologies consistently achieve higher rates of recall[59] and precision[60] in document review than human lawyers, leading to increased use and unquestionable impacts on the demand for lawyer labor.[61] Because of this, we characterize predictive coding technologies as having a strong employment effect on discovery practice.

Nevertheless, we note that predictive coding cannot completely displace lawyer labor in discovery practice for several reasons. First, attorneys must still classify a sample of documents and train the system’s parameters, leading to up-front costs that render the system inefficient for cases that do not entail large volumes of documents. Second, lawyers who have an understanding of the case, the implicated document sets, and the variety of available predictive coding

[54] These characteristics are called “features” of the document. As noted above, this estimation might now be done using a probabilistic language model and a neural net that would automatically extract relevant features as part of the estimation. In practice, the lawyers test the model on subsequent sample sets in an iterative process that continues until the lawyers are satisfied that the program is appropriately classifying documents.

[55] *See* Moore v. Publicis Groupe, 287 F.R.D. 182, 193 (S.D.N.Y. 2012), *adopted sub nom.* Moore v. Publicis Groupe SA, No. 11 Civ. 1279(ALC)(AJP), 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012) (“Computer-assisted review now can be considered judicially-approved for use in appropriate cases.”).

[56] *See, e.g.*, KCURA, https://www.kcura.com/about-us/our-company/ [https://perma.cc/6KRX-6FXM] (last visited Apr. 2, 2017).

[57] Telephone conversation with Maura Grossman & Gordon Cormack (Jan. 13, 2016).

[58] That statistical model, or algorithm, then ranks each document in the complete set for the likelihood that it is responsive. The top-ranking documents are “skimmed” off the top and coded by the supervising lawyers. The algorithm is then retrained using all documents that have been coded, and re-applied to the entire document set, less those that have already been set aside as responsive. This process continues until so many of the responsive documents have been identified and set aside that the highest scoring documents returned by the algorithm no longer appear responsive.

[59] Recall is the fraction of all responsive documents that the algorithm identifies as responsive.

[60] Precision is the fraction of all documents that the algorithm identifies as responsive that are actually responsive.

[61] *See, e.g.*, Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient than Exhaustive Manual Review*, 17 RICH. J.L. & TECH. 1, 3 (2011); Herbert L. Roitblat et al., *Document Categorization in Legal Electronic Discovery: Computer Classification vs. Manual Review*, 61 J. AM. SOC’Y FOR INFO. SCI. & TECH. 70, 70, 74–75 (2010).

technologies are still needed to select the most appropriate products and protocols given the implicated data sets, and, if need be, to defend those choices in court.[62] Finally, the typical algorithm assigns each document an ex ante probability of responsiveness, requiring lawyers to hand-classify those documents with intermediate probabilities.[63]

6. DUE DILIGENCE (MODERATE EMPLOYMENT IMPACT)

Due diligence entails investigating and reviewing a particular client, entity, or situation to ensure comprehensive understanding of all factual and legal issues relevant to a proposed deal or transaction. Part of this, which we address here, entails reviewing documents; part, which we address below, entails investigating implicated facts and interviewing relevant parties.

The document review of due diligence differs in critical respects from the document review of discovery practice, addressed above. The former is a structured task in which a single pattern of linguistic features is used to classify an entire set of documents. The latter encompasses a structured component (locating and, where possible, analyzing the contractual obligations of a potential partner or acquisition) and an unstructured component (searching for unexpected or surprising information from a diverse set of documents).

Technology firms have worked, with some success, to automate the structured component of due diligence. Apogee Legal[64] and Kira Systems[65] have developed software that crawls a company's network to identify vendor and sourcing contracts, customer agreements, software licenses, and leases. Notably, these programs are only effective if they can be trained on a sufficient volume of similar documents. Seeking to overcome this limitation, Kira Systems has also developed a platform that flags particular clauses (for example, assignment clauses) in a diverse array of contracts and other documents.[66] The software contains a standard list of target clauses (each in multiple wordings), and additional target clauses can be specified by the user. The software uses machine learning techniques, similar in purpose to LSA, to automate the judgment that two sets of words have similar meaning.[67]

Other aspects of due diligence review resist automation because they involve searching for unanticipated information—for example, a contractual relationship

[62] Some versions classify documents primarily by reference to words; some by reference to word fragments (i.e., four character combinations); some by reference to metadata; and some by reference to a combination. Moreover, and as just described, some protocols begin with a random sample of documents, while others focus on clearly relevant ones.

[63] We return to this point *infra* Part II.C.

[64] APOGEE LEGAL, https://apogeelegal.com/ [https://perma.cc/3MGG-7L28] (last visited Apr. 2, 2017).

[65] KIRA, *supra* note 44.

[66] Interview with Noah Waisberg & Steve Obenski, Kira Systems (Jan. 13, 2016).

[67] *See How Kira Works*, KIRA, https://kirasystems.com/how-it-works/contract-analysis [https://perma.cc/7NVW-JM2Z] (last visited Apr. 2, 2017).

with a party that might violate a provision of law.[68] This limitation points to a broader issue. The human mind can draw correct inferences from very limited information,[69] allowing a human lawyer to use context, analogies, and common sense to identify a contractual reference as a problem even if the reference was unanticipated. By contrast, current machine learning software will identify the reference as problematic only if something related to the problematic language was anticipated and included in the training data.

Over time, machine learning software can improve through use as incorrect responses to previously unseen questions are corrected. This is particularly true if the software is marketed as a service sold to multiple customers[70] so that all corrections can be pooled in a single version of the software. For the present, however, these limitations remain. We therefore characterize due diligence as being subject to moderate employment effects.

7. DOCUMENT DRAFTING (MODERATE EMPLOYMENT IMPACT)

Document drafting is the development of legal documents such as deeds, contracts, wills, and trusts, that reflect the intent and agreement of the parties as accurately and unambiguously as possible. Showing that this task is, at base, structured, lawyers have long used templates in drafting these documents. Since the advent of personal computing, they have been storing these templates, often referred to as forms, on desktop computers.

More recently, a number of applications have enabled automated customization of basic forms.[71] For example, a lawyer will enter information about a client's wishes regarding disposition of her estate and the computer will produce a customized will for the lawyer to review. These programs can certainly increase lawyers' efficiency, but given lawyers' prior and longstanding reliance on forms in legal drafting, we estimate that new software will only have a moderate impact on lawyer labor within firms.[72]

A more distinct innovation, which may have a more distinct impact on lawyer employment (though outside of large firms), is the business model of online service providers that market templates directly to consumers. LegalZoom, for example, allows a consumer to obtain a number of legal documents from its website (including wills, powers of attorney, business filings, and bankruptcy or

[68] Telephone Interview with Nathalie Hofman, Managing Dir., Huron Legal, Huron Consulting Grp. Inc. (July 21, 2015).

[69] *See, e.g.*, *Linda Smith—The Visual Side of Early Object Name Learning (1 to 2 year old toddlers)*, YOUTUBE (Oct. 5, 2015), https://www.youtube.com/watch?v=zDZIpqJkNe8 [https://perma.cc/7DHH-PS6Y].

[70] The alternative is that each customer operates a free-standing software package.

[71] Automated document drafting programs are frequently incorporated into document management software used by law firms. *See supra* note 40.

[72] See *infra* note 150 and accompanying text for discussion of another frequently discussed innovation, blockchain contracts.

divorce petitions)[73] by indicating the document in which he or she is interested and answering a series of document-specific questions. Based on the consumer's answers, the website produces a completed and customized document.

We return to online service providers below. For now, we simply note that any employment impacts on lawyers, which we characterize as moderate, will be felt among solo practitioners and lawyers in small firms.

8. LEGAL WRITING (WEAK EMPLOYMENT IMPACT)

Legal writing, as distinct from legal document drafting, is the development of written work that characterizes the state of the law and/or its application to a particular factual situation. Whether objective or persuasive, legal writing is very difficult to automate. Commentators cite automated Associated Press summaries of baseball games and corporate earnings reports to argue that this will soon change[74] and that automated legal briefs are right around the corner, but the analogy does not hold. Extracting and summarizing relevant information about a baseball game or a company's reported financial situation is a structured task—a baseball game can be largely reconstructed from the pitch-by-pitch game feed, and earnings reports have relatively structured and standard formats. Once the game (or the earnings report) has been reconstructed, writing the summary involves a structured selection and listing of prewritten phrases with insertion of particular proper nouns (e.g., players' names).[75]

Notwithstanding recent innovations by Ross Intelligence, discussed below, to respond to a legal query with a short memo, the vast majority of legal writing is insufficiently structured to be automated in this way. Whereas a sports writer covers a settled game structure and a final definitive score, a lawyer often writes amidst indeterminacy. Certainly, parts of a brief are standard and predictable—for example, the preliminary and concluding material, and the statement and explanation of relevant standards of review. But much legal writing requires conceptual creativity and flexibility that computers do not currently exhibit. The analysis section of a legal brief requires a complex interplay between law and fact, in which the law that governs is determined by the facts, while the relevant facts are determined by the governing law. The use of precedent, while second nature for a lawyer, is exceedingly difficult (and currently impossible) to model

[73] *About Us*, LEGALZOOM, https://www.legalzoom.com/about-us [https://perma.cc/9KF5-684B] (last visited Apr. 2, 2017).

[74] McGinnis & Pearce, *supra* note 2, at 3051.

[75] Note also that these short articles are usually directed at readers with limited information demands: a New York newspaper will contain an extensive, non-automated article on a Yankees game while using Associated Press summaries to report on out-of-town games. For example, Automated Insights's website describes producing stories in four steps: "1. Add your data; 2. Write your template; 3. Preview your stories; 4. Publish your stories." *Here's How Wordsmith Works*, AUTOMATED INSIGHTS, https://automatedinsights.com [https://perma.cc/3PHK-TBHV] (last visited Apr. 2, 2017).

for a computer. A single case can be used to support two opposing positions; arguing for one as opposed to the other requires an ability to contextualize the case in a line of precedent, and to distinguish between a binding holding and non-binding dicta. Often, an effective legal argument also requires the ability to transplant concepts from one area of law to another in order to argue for a novel legal theory or change in the law. These unstructured and opaque conceptual tasks lay beyond the current capacity of computers. We therefore categorize legal writing as currently subject to weak employment impacts.

9. LEGAL RESEARCH (MODERATE IMPACT)

Vern R. Walker, co-organizer of the first conference on argument mining, offers a useful perspective on the evolution of automated legal research:

> The ultimate goal of legal research by lawyers and decision makers is to find arguments and reasoning reported in the past, so that they can evaluate the likelihood of success of those and similar arguments, and can generate new arguments to use in future cases. I think that this suite of tasks is also the ultimate goal of software analytics, such as Westlaw, FastCase, Ross, etc. That's the direction in which we are all headed with automating legal research.[76]

From an artificial intelligence perspective, legal research is a problem in information extraction, where the critical design element involves linking a user's search query to the best available answers. Early innovations in automated legal research came from computerized legal databases such as Westlaw and Lexis. A user of Westlaw and Lexis could begin with a key word search, but keyword searching is frequently both under and over-inclusive.[77] The innovation of both services was to offer an indexing tool—an improved link between query and legal case. Constructing these indexing tools involves a significant amount of human processing, however, and is therefore expensive.[78] Because of the difficulty of automating text summarization, discussed below, humans write a summary headnote for each case filed in the system.[79]

For Lexis, humans then use these headnotes to classify cases into the Lexis Topic system; for Westlaw, a machine learning algorithm links the headnotes to

[76] Interview with Vern R. Walker, Professor of Law, Dir., Research Lab. for Law, Logic, & Tech., Hofstra Law Sch. (June 29, 2016).

[77] A user could refine the keyword-searched database so as to examine only cases in a relevant jurisdiction or time period.

[78] In economic terms, the indexing is a large fixed cost, which explains why the system is constructed by a small number of providers and sold as a service.

[79] *See* Dan Jurafsky & Christopher Manning, *Natural Language Processing*, STANFORD ONLINE (June 13, 2012), http://online.stanford.edu/course/natural-language-processing [https://perma.cc/5UN5-NVDD].

the West Key typology codes.[80]

FastCase, a 2010 entrant to the legal research market, abandoned the index system and instead links a query to cases primarily by a combination of citation frequency and relative strength of the citation.[81] The algorithm functions similarly to Google's algorithm for searching the web,[82] and like Google's algorithm, presents results ranked in terms of estimated relevance.[83] New versions of Lexis and Westlaw are incorporating relevancy rankings as well, based on a combination of features such as past search patterns, document characteristics, and matching terms.

In Walker's framing, Lexis, Westlaw, and FastCase respond to legal queries by retrieving citations to complete cases—full documents that contain legal arguments or that set forth or summarize existing law. More recent software research tools focus on retrieving something closer to the underlying arguments themselves. One application gaining substantial publicity is Ross Intelligence, an IBM Watson-based question and answer (Q/A) system that accepts natural language questions rather than keywords and that retrieves relevant passages rather than entire cases.[84]

Assume a user enters the following question on bankruptcy law: "When can a debtor reject a collective bargaining agreement?" Roughly speaking, a Watson-based Q/A system answers this question in three phases.[85] A parsing module determines what the question is about (i.e., the entities of interest—debtor, collective bargaining agreement, and the relationship among entities (rejection)). A second module retrieves potentially relevant passages from the system's database. A third module ranks the retrieved passages, assigning each passage the probability that it represents the best answer. The second and third modules rest on LSA and related techniques, discussed above, to measure the similarity of candidate passages to the question.[86]

[80] *See* Susan Nevelow Mart, *The Relevance of Results Generated by Human Indexing and Computer Algorithms: A Study of West's Headnotes and Key Numbers and LexisNexis's Headnotes and Topics*, 102 L. LIBR. J. 221, 223–24 (2010).

[81] *See What is Fastcase?*, FASTCASE, http://www.fastcase.com/whatisfastcase/ [https://perma.cc/W24H-KQDP] (last visited Apr. 2, 2017).

[82] *See How Does Google Search the Web*, YOUTUBE (Apr. 23, 2012), https://www.youtube.com/watch?v=KyCYyoGusqs [https://perma.cc/6YRH-FWDC].

[83] Initial versions of Westlaw and Lexis listed results in reverse chronological order or frequency of keywords.

[84] ROSS INTELLIGENCE, *supra* note 4.

[85] "Watson" is actually a suite of applications. The configuration of Watson that won *Jeopardy!* was comprised of sophisticated natural language processing capabilities and an ability to access multiple databases (including Wikipedia) to search for answers. Developers of more recent Watson applications often retain the natural language processing capabilities, but build their own databases.

[86] For a more complete description of Watson's question answering architecture, see David Ferrucci et al., *Building Watson: An Overview of the Deep QA Project*, 31 AI MAG. 59 (2010); Dan Jurafsky & James H. Martin, Speech and Language Processing (3d ed. draft Jan. 2017), https://web.stanford.edu/jurafsky/slp3/ [https://perma.cc/PVN8-3S38].

The system is modeled using neural nets, statistical models with multiple non-linear interactions among variables. Such models are statistically complex, but at base similar to Equation 1 above. The neural net takes information inputs—the characteristics of a particular passage—which it then processes into an output—the probability that the passage is the best answer to the question.

When a user builds a new system, much of the language-parsing module is prepackaged. But the retrieval and ranking neural nets must be trained through supervised learning, and so, like Westlaw and Lexis, require a substantial initial effort.[87] The training process begins by populating the system's database with legal documents that have been broken into passages by human experts. The experts essentially annotate the database by attaching to each passage a set of natural language practice questions such that the passage is the correct answer for each of the attached questions. Each practice question must be worded in multiple ways to reduce the likelihood that the system will fail to recognize a user's question as having the same meaning as an already-processed question. The system is then trained using an iterative process of posing a question, noting whether the system's suggested passage is correct or incorrect, and adjusting the neural net's parameters (roughly equivalent to β's in Equation 1) accordingly. The process is complicated by the fact that questions are often imprecisely expressed. For example, in the question above, does "When" mean the user expects an answer in the form of a time period ("after ninety days . . .") or a set of conditions ("if the collective bargaining agreement contains . . .").

If experts could anticipate precisely how every question would be asked, there would be no need for machine learning to estimate statistical links—each specifically worded question could be tied directly to its answer. Once in operation, however, the system will receive many questions that are more or less similar but not identical to the questions on which it has been trained. Consider the following example: "Can a debtor reject a collective bargaining agreement where debtor is a city that filed for Chapter 9 bankruptcy and previously attempted to negotiate with a private union before rejecting its collective bargaining agreement?"

This question, both specific and complicated, is unlikely to have been part of the system's training. And yet, it has linguistic features in common with the training question discussed above, as well as other linguistic features that may be able to activate other links: the debtor is a city, the city is in Chapter 9 bankruptcy, a time relationship in which negotiations occurred before the collective bargaining agreement was rejected. Using all relevant links, there is a chance that

[87] As is the case with Westlaw and Lexis, the large initial cost means such customers access such question/answering systems by purchasing them as a service rather than building their own system. The corollary is that the system must be focused on a set of questions/answers that are of potential interest to a broad set of customers. Current versions of Ross are focused on bankruptcy law.

the system will produce a relevant and responsive set of paragraphs for this question, which it has not previously seen.

Accordingly, an operational Q/A system will likely confront questions it has not seen before. Questions involving abstract concepts and analogies can be particularly complex to analyze. These problems can be reduced over time with continuous training that refines question-answer links, but such training requires use by senior attorneys and not just young associates who may be too inexperienced to spot the system's errors.

As noted above, Ross's Q/A system now offers yet another innovation—an ability to answer certain legal questions with well-organized two-page memos rather than relevant passages.[88] Ross officials are understandably reluctant to discuss their technology, but Ross's close association with IBM makes it reasonable to speculate that Ross's memos rely on a variant of the answers produced by IBM's Debater System.[89] The Debater System is part of the developing field of argument mining, the subject of Walker's quote above. Argument mining is an area of natural language processing that draws on a text corpus—for example, Wikipedia entries or sections of *Collier on Bankruptcy*—to create a short essay supporting or opposing a stated proposition. To set up the software, human reviewers first review the corpus to identify specific topics and label three types of passages associated with each topic: background, claims, and evidence.[90] Setting up the software also requires constructing an essay template in which selected passages will be inserted into background, claim, and evidence fields to form the completed document. When the system is presented with a question, the software selects candidate passages based on topic and ranks them for their responsiveness to the question—a process broadly similar to judging the similarity between pieces of text. The highest ranked background-claim-evidence sets are inserted into template slots to form the essay.[91]

Strictly speaking, this is not a fully automated system because it initially requires humans to label the corpus. Humans label the corpus only once, however, regardless of the number of users. Still, in considering the employment impacts of this and all legal research tools, it is important to recognize the substantial remaining human role in defining and directing research. This role leads us to characterize the impact of automation on legal research as moderate

[88] Susan Beck, *Inside ROSS: What Artificial Intelligence Means for Your Firm*, LAW.COM (Sept. 28, 2016), http://www.law.com/sites/almstaff/2016/09/28/inside-ross-what-artificial-intelligence-means-for-your-firm/?slreturn=20170114162046 [https://perma.cc/NHJ4-PB4W].

[89] *IBM Debating Technologies*, IBM, http://researcher.ibm.com/researcher/view_group.php?id=5443 [https://perma.cc/EB8B-42AX] (last visited Apr. 2, 2017).

[90] *See* Ehud Aharoni et al., *A Benchmark Dataset for Automatic Detection of Claims and Evidence in the Context of Controversial Topics*, at 64–65 (Proceedings of the First Workshop on Argumentation Mining, Ass'n for Computational Linguistics, June 26, 2014), http://www.aclweb.org/anthology/W14-2109 [https://perma.cc/AP9U-XFH6].

[91] *See id.*

notwithstanding impressive advances in legal research tools. Consider, for example, the nature of a case law search, which frequently begins with an initial set of controlling cases. As Susan Mart writes:

> [I]t is rare that the facts of those cases are so close to the facts of the client's case that your research is complete. The second part of the research project then begins—the search for case-specific relevant authority. The researcher needs to find other cases, similar in legal conclusions and more similar factually to the client's case. This search for more specifically relevant primary law can be called "level two research." The researcher uses the major and controlling cases in the relevant area of the law (however located) as seed documents to link forward through headnotes, key numbers, KeyCite, and Shepard's or backward through headnotes, key numbers, and the cases cited in the seed cases. This type of forward and backward searching from seed documents is instrumental for finding "application cases"—cases that have only marginal value as support for an abstract proposition of law, [but] have great value in their application of the proposition to facts similar or analogous to the facts of your own case.[92]

Mart describes an iterative process in which a lawyer specifies the parameters for a search, which the software then performs. It is therefore the search that has been automated, not the entire task of researching precedents. A similar logic applies to question and answering systems. They can automate an actual search, often more effectively than Westlaw or Lexis, but they cannot automate the designation of search parameters. That work remains for lawyers—most often, for associates.

10. LEGAL ANALYSIS AND STRATEGY (MODERATE EMPLOYMENT IMPACT)

Legal analysis and strategy entails the exercise of legal judgment in evaluating a situation and planning accordingly. Two advances in automation have made inroads on this work, which was traditionally thought of as immune to automation. The first is prediction. In recent years, software such as Ravel Law and Lex Machina have collected and analyzed massive amounts of data on judges and their decisions, producing data-driven statistical models, similar in structure to Equation 1, that are often more accurate than human prediction.[93] Automated prediction of jury decisions has proven far more elusive, however, and even with

[92] Mart, *supra* note 80, at 222 (footnotes omitted).

[93] For example, a 2015 press release explains: "By analyzing millions of legal documents, Ravel provides strategic insight into an array of factors that affect a judge's decision-making." *Ravel Law Announces Unprecedented Judge Analytics Offering*, PRWEB (Apr. 16, 2015), http://www.prweb.com/releases/2015/04/prweb12656883.htm [https://perma.cc/SHC9-VB2J]; *see also What We Do*, LEX MACHINA, https://lexmachina.com/what-we-do/ [https://perma.cc/S9PS-K5N5] (last visited Mar. 3, 2017) ("We mine litigation data, revealing insights never before available about judges, lawyers, parties, and patents, culled from millions of pages of IP litigation information. We call these insights Legal Analytics®, because analytics involves the discovery and communication of meaningful patterns in data.").

respect to bench trials, a significant human role remains in interpreting the data and formulating advice for clients. Prediction software and data analytics also offer the possibility of law firms getting a better understanding of the risks and costs associated with large cases. While such knowledge may allow a law firm to run with greater efficiency, it has ambiguous employment effects.

A second area of progress in computerized legal reasoning is the development of expert systems. Built on platforms by Neota Logic[94] and others, expert systems organize and present a specific, narrow legal task as a structured dialog with the user. Once constructed, these systems can be scaled to many users, delivering legal reasoning at a much lower cost than if a human lawyer responded to each user separately. A recent, much discussed example is DoNotPay, an expert system developed by a 19-year-old British student that helped British drivers overturn at least 160,000 parking tickets.[95]

As of now, such systems can only be constructed for repetitive and fairly narrow tasks under specific bodies of law—for example, compliance with the Foreign Corrupt Practices Act.[96] As the parking ticket example suggests, not all users of expert systems would have otherwise used a lawyer. To the contrary, expert systems are often described as a way for a law firm to offer a low-cost service to potential clients for addressing low-stakes cases. The hope is that the client then turns to the firm to deal with more complex situations. Because of this, we characterize the employment impacts of automation on legal analysis and strategy as moderate.

11. ADVISING CLIENTS AND OTHER COMMUNICATIONS/INTERACTIONS (WEAK EMPLOYMENT IMPACT)

For current purposes, we group two very different sets of tasks—advising clients and communicating and interacting—with all others. Although the work of these two categories is distinct, it requires a significant amount of unstructured human interaction, rendering both categories of work subject to weak employment impacts.

With respect to client advising, computers have made significant progress in two areas. They have made it easier for individuals to access relevant legal information, whether through free online legal databases or issue-specific

[94] NEOTA LOGIC, http://www.neotalogic.com [https://perma.cc/FRG3-6DFK] (last visited Apr. 2, 2017).

[95] Samuel Gibbs, *Chatbot Lawyer Overturns 160,000 Parking Tickets in London and New York*, GUARDIAN (June 28, 2016), https://www.theguardian.com/technology/2016/jun/28/chatbot-ai-lawyer-donotpay-parking-tickets-london-new-york [https://perma.cc/46QT-JK6U].

[96] *See, e.g.*, *Foley & Lardner LLP Selects Neota Logic Technology Platform to Power Award-Winning Foley Global Risk Solutions Offering*, NEOTA LOGIC (2016), https://cdn2.hubspot.net/hubfs/453162/Foley%20Lardner.pdf?submissionGuid=c6c807c3-3154-40c7-af4c-5ba8c6315cd1 [https://perma.cc/B7MA-58G7].

web-based applications.[97] They have also made progress in an area just noted—prediction.

For at least three reasons, however, most client advising remains outside of the current domain of automation. First, legal prediction software programs address only courts and case law, but lawyers must routinely predict many other things, such as how an opponent will react to a settlement offer or how an agency will interpret a regulation. Second, many clients want more than a series of statistical probabilities. They want a lawyer's judgment and assurances as to what course of action will most effectively serve their short and long-term interests. Some clients want this for their own comfort; others want it to reassure affected constituents; still others want it for purposes of a potential advice-of-counsel defense.[98] Third and most importantly, effective advising encompasses more than prediction. It requires a lawyer to understand a client's situation, goals, and interests;[99] to think creatively about how best to serve those interests pursuant to law; and sometimes, to push back against a client's proposed course of action and counsel compliance.[100] These are things that frequently require human interaction and emotional intelligence[101] and cannot, at least for the time being, be automated.

More broadly, the vast majority of a lawyer's personal interactions—with clients as well as with all others—continue to require spontaneity, unstructured communication, and emotional intelligence. Examples are plentiful: A lawyer may need to push a client to execute a will; spend hours interviewing a criminal defendant to develop enough trust to elicit full information; or read a deponent's facial expressions and body language to determine how to proceed with questioning. Moreover, many individual clients report that a lawyer's trustworthi-

[97] *See, e.g.*, Tanina Rostain et al., *Thinking Like a Lawyer, Designing Like an Architect: Preparing Students for the 21st Century Practice*, 88 CHI.-KENT L. REV. 743 (2013) [hereinafter Rostain et al., *Thinking Like a Lawyer*].

[98] Many clients may want a lawyer's advice as a means of avoiding what behavioral economists refer to as "regret"—the guilt and responsibility that can accompany a wrong decision in an uncertain situation. *Cf.* Richard H. Thaler*, Toward a Positive Theory of Consumer Choice*, 1 J. ECON. BEHAV. & ORG. 39, 54 (1980) (observing that one reason doctors look for second opinions is to share responsibility and reduce regret for diagnoses that may turn out to be wrong).

[99] *See* Katherine R. Kruse, *Beyond Cardboard Clients in Legal Ethics*, 23 GEO. J. LEGAL ETHICS 103, 104 (2010) [hereinafter Kruse, *Beyond Cardboard Clients*]; Katherine R. Kruse, *The Promise of Client-Centered Professional Norms*, 12 NEV. L.J. 341, 346 (2012) [hereinafter Kruse, *Client-Centered Norms*]; Marc Lauritsen, *Liberty, Justice, and Legal Automata*, 88 CHI.-KENT L. REV. 945, 954 (2013); William H. Simon, *The Ideology of Advocacy: Procedural Justice and Professional Ethics*, 1978 WIS. L. REV. 29, 53.

[100] *See generally* DEBORAH L. RHODE, IN THE INTERESTS OF JUSTICE (2000) [hereinafter RHODE, INTERESTS OF JUSTICE]; Robert W. Gordon, *A New Role for Lawyers?: The Corporate Counselor After Enron*, 35 CONN. L. REV. 1185 (2003) [hereinafter Gordon, *New Role for Lawyers?*]; Tanina Rostain*, Ethics Lost: Limitations of Current Approaches to Lawyer Regulation*, 71 S. CAL. L. REV. 1273, 1274–75 (1998) [hereinafter Rostain*, Ethics Lost*]; W. Bradley Wendel, *Professionalism as Interpretation*, 99 NW. U. L. REV. 1167, 1171–72 (2005) [hereinafter Wendel, *Professionalism as Interpretation*].

[101] Remus, *Reconstructing Professionalism*, *supra* note 10, at 25–29.

ness and ability to provide a close and personal relationship are among the most important traits they look for from a lawyer.[102] For the time being, therefore, we think the impact of automation on the areas of client counseling and interactions with third parties will remain weak.

12. FACT INVESTIGATION (WEAK EMPLOYMENT IMPACT)

Fact investigation, similarly dependent on unstructured communications, is also subject to weak employment impacts. Some aspects of the task can be automated—for example, software can usefully pull together vast amounts of online data regarding a client or opponent, and some lawyers and legal aid clinics automate initial client intake. For the most part, however, factual investigation resists automation. It frequently entails interviews in which significant amounts of information may be transmitted nonverbally, in ways a computer would have difficulty detecting, at least for now. It also requires flexibility from a lawyer, beyond the capacity of a computer, in adjusting the relevant questions as new information is discovered.

13. NEGOTIATION (WEAK EMPLOYMENT IMPACT)

Traditionally, negotiation also required personal interaction and effective use of emotion. Negotiation experts have long theorized that skill in reading an opponent's emotions allows a negotiator to achieve greater understanding of the opponent's interests and concerns, to assess risk more accurately, and to deploy negotiation tactics more effectively.[103] Online dispute resolution programs are rendering these human skills unnecessary in a small but growing category of cases, however.[104] An example is Modria, a California firm that markets online dispute resolution to e-commerce companies.[105] Its website describes that it

[102] *See* COREY S. SHDAIMAH, NEGOTIATING JUSTICE: PROGRESSIVE LAWYERING, LOW-INCOME CLIENTS, AND THE QUEST FOR SOCIAL CHANGE (2009) (citing interviews of clients expressing that friendship and trust were at the forefront of what they wanted from lawyers); Marcus T. Boccaccini et al., *Client-Relations Skills in Effective Lawyering: Attitudes of Criminal Defense Attorneys and Experienced Clients*, 26 LAW & PSYCHOL. REV. 97, 110–11 (2002) (citing a poll in which clients ranked obtaining clients' opinions, spending time with clients before court, and keeping clients informed of their cases as among the things they cared most about in a lawyer; also citing evidence that inmates cared more about a lawyer who cared about them, would be honest, and would spend time with them before their court date than about the lawyer's skills); Marcus T. Boccaccini & Stanley L. Brodsky, *Characteristics of the Ideal Criminal Defense Attorney from the Client's Perspective: Empirical Findings and Implications for Legal Practice*, 25 LAW & PSYCHOL. REV. 81, 98 (2001); Anne E. Thar, *What Do Clients Really Want? It's Time You Found Out*, 87 ILL. B.J. 331 (1999).

[103] *See* Kimberlyn Leary et al., *Negotiating with Emotion*, HARV. BUS. REV. (Jan.–Feb. 2013), https://hbr.org/2013/01/negotiating-with-emotion [https://perma.cc/F7CL-PUL4].

[104] *See* Richard Susskind & Matthew Levy, *Likely Developments in ODR*, CTS. & TRIBUNALS JUDICIARY (Feb. 16, 2015), https://www.judiciary.gov.uk/publications/likely-developments-in-odr/ [https://perma.cc/U4V5-68S8]; *see also* Hornsby, *supra* note 11.

[105] *About Us*, MODRIA, http://www.modria.com/about-us/ [https://perma.cc/MD4D-PFVR] (last visited Apr. 2, 2017).

gathers relevant information regarding the dispute, summarizes areas of agreement and disagreement, and makes suggestions for resolving the issue.[106] It does so through deductive instructions, rendering negotiation (as lawyers understand the task) unnecessary.[107]

Currently, the approach is used primarily for small disputes, but Modria is expanding into larger and more complicated types of disputes.[108] A number of other companies are developing similar products,[109] while legal reform groups are encouraging courts to increase efficiency and manage dockets through use of such products.[110]

Additional new technologies are emerging to aid lawyers in negotiating by, for example, analyzing and representing the overlap between two parties' preferences.[111] Such programs address one or at most two issues, and their resolution is constrained by the parties' stated initial preferences. They nevertheless suggest that computers may eventually play a larger role in aiding, if not replacing, lawyers' negotiating work.

In theory, online dispute resolution and expert systems could also fall into the category of heavy employment effects given that when used, they entirely replace lawyers (and in the case of online dispute resolution, judges as well). Their impact on lawyer employment may be significant in the future, but we estimate it is minimal at present. The disputes that these systems resolve are generally small stakes e-commerce issues, for which it would not be economically feasible to hire

[106] *How it Works*, MODRIA, http://www.modria.com/how-it-works [https://perma.cc/4LRF-RH9H] (last visited Apr. 2, 2017).

[107] For example, a deductive instruction could read: ("If (Customer is Low Risk) and (Dispute Amount is less than ten dollars) and (Customer Disputes Filed Account Lifetime is (0)) then (Authorize Full Refund) and (Close Case).").

[108] Eric Johnson, *Modria Wants You to Settle Your Workplace Problems (and Even Patent Disputes) Online*, ALL THINGS D (Nov. 24, 2012), http://allthingsd.com/20121124/modria-wants-you-to-settle-your-workplace-problems-and-even-patent-disputes-online/ [https://perma.cc/DC8L-Q6GX]; *see also Modria—The Operating System for ODR (video extract)*, CTS. & TRIBUNALS JUDICIARY (Feb. 16, 2015), https://www.judiciary.gov.uk/publications/modria-the-operating-system-for-odr-video-extract/ [https://perma.cc/6UZF-VP3J] ("[O]ur goal is to be the operating system for online dispute resolution. So any kind of dispute, no matter how complicated or how simple, how high volume or low volume, we can use these building blocks at Modria to build an appropriate resolution path for that dispute. So that's our objective.").

[109] *See, e.g.*, Graham Ross & Beth Silver, *Case Studies*, CTS. & TRIBUNALS JUDICIARY (Feb. 16, 2015), https://www.judiciary.gov.uk/publications/case-studies/ [https://perma.cc/K87F-RFQE].

[110] *See, e.g.*, Civil Justice Council Online Dispute Resolution Advisory Grp., *Online Dispute Resolution for Low Value Civil Claims*, at 3 (Feb. 2015), https://www.judiciary.gov.uk/wp-content/uploads/2015/02/Online-Dispute-Resolution-Final-Web-Version1.pdf [https://perma.cc/KJP6-LJKB] (recommending a new Internet-based court service, which would offer three services: Online Evaluation, which would help users to understand and evaluate their potential claims; Online Facilitation, which would facilitate early resolution of disputes without the involvement of a judge; and Online Judges, who would decide parts or all of cases through structured online pleading).

[111] Keith Winstein, for example, has shown that some telecom-related negotiations on access prices could be solved by an online auction. *See Keith Winstein's Homepage*, STANFORD COMPUT. SCI., http://cs.stanford.edu/keithw/ [https://perma.cc/5JLW-TM3J] (last visited Apr. 2, 2017).

a lawyer and litigate (such that lawyer labor is not being replaced).[112] Similarly, expert systems are generally directed at reaching new markets rather than improving efficiency in existing tasks. For example, a law firm might offer subscriptions to an expert system covering aspects of tax compliance to clients who otherwise might not consult a lawyer,[113] increasing the firm's business but not displacing any lawyers.[114] For the time being, therefore, we characterize the impact of these services on lawyer employment as weak.

14. COURT APPEARANCES AND PREPARATION (WEAK EMPLOYMENT IMPACT)

A final category of work, courtroom advocacy, is distinct from the others insofar as even the most fervent technology advocates are not predicting near-term automation. In part, this is because the policies and restrictions of unauthorized practice of law rules operate at their strongest in the courtroom. More fundamentally, it is because effective advocacy requires emotional engagement with the decision-maker.[115] As two experienced advocates explain:

> An inexperienced trial lawyer's dull and confusing closing argument in a complex business dispute will create negative feelings of boredom and frustration in the minds of the jurors . . . an accomplished advocate can communicate to the juror the facts of the identical dispute in a way that will evoke positive emotions about justice and fairness in the marketplace.[116]

It is not only in arguments to a jury that emotion is critical. The emotions a lawyer deploys to persuade a judge may differ from those designed to persuade a jury, but emotion is a critical spur to all action and decision-making.[117] And yet, the field of affective computing is nowhere near enabling computers to foster, recognize, and respond to the full range of human emotions.

* * *

Table 2 summarizes the foregoing discussion by restating the time usage data of Table 1, while also indicating the employment effects on lawyers of automation of each task.

[112] *See supra* notes 93–96 and accompanying text.

[113] The subscription might include a limited amount of access to the firm's lawyers on questions the system cannot answer and the firm would keep track of such questions in order to update the system.

[114] The existence of markets for such systems points to the relationship between automation and proportionality, discussed below. *See infra* Part II.C.5.

[115] *See, e.g.*, LANE COOPER, THE RHETORIC OF ARISTOTLE (1st ed. 1960); RICHARD DU CANN, THE ART OF THE ADVOCATE: AN INCISIVE EXAMINATION OF THE ROLE OF THE ADVOCATE IN TODAY'S LEGAL SYSTEM 156 (1980); PAM WRIGHT & PETE WRIGHT, FROM EMOTIONS TO ADVOCACY (2003).

[116] John C. Shepherd & Jordan B. Cherrick, *Advocacy and Emotion*, 3 J. ASS'N LEGAL WRITING DIRECTORS 152, 152 (2006) (originally published as 138 F.R.D. 619 (1991)).

[117] *Id.* at 153.

TABLE 2
PERCENT OF INVOICED HOURS SPENT ON VARIOUS TASKS, GROUPED BY ESTIMATED EXTENT OF COMPUTER PENETRATION

Task	Tier One Firms	Tier Two–Five Firms
Strong Employment Effects	**4.1%**	**3.6%**
Document Review	4.1%	3.6%
Moderate Employment Effects	**39.7%**	**40.4%**
Case Administration and Management	3.7%	5.6%
Document Drafting	5.0%	4.0%
Due Diligence	2.0%	3.4%
Legal Research	0.5%	0.4%
Legal Analysis and Strategy	28.5%	27.0%
Light Employment Effects	**56.0%**	**55.7%**
Document Management	0.4%	0.7%
Fact Investigation	9.2%	9.6%
Legal Writing	11.4%	17.7%
Advising Clients	9.3%	3.2%
Other Communications/ Interactions	8.8%	5.0%
Court Appearances and Preparation	13.9%	14.5%
Negotiation	3.0%	5.0%
Totals**	99.8%	99.7%

** Percentages may not sum to 100% due to rounding.

Note that only 4.1 percent of lawyers' time at Tier 1 firms, and 3.6 percent of time at Tier 2–5 firms was billed to tasks where automation potentially has strong employment effects. One could argue that these low percentages reflect the impact that predictive coding has already had in automating document review. However, predictive coding was not widely used until it was officially blessed by a federal judge in 2012, and in Sky Analytics data for 2012, lawyers at Tier 1 firms billed only six percent of their time to document review.

More likely, the low percentage is explained by two factors. First, document review in our typology covers only discovery practice, not due diligence (which, as described above, is harder to automate). Accordingly, associates in departments other than litigation would not devote any of their time to the task. Second, as noted earlier, clients have been pressuring law firms for over a decade to hold down litigation costs through outsourcing, offshoring, and using contract attorneys to perform document review.[118] These pressures intensified following the 2008 financial collapse, when a shift in supply versus demand empowered clients to insist on cost-cutting measures, including outsourcing and the exclusion of junior associates from their matters.[119] Thus, the task may already have been pushed out of the domain of firm lawyers' work by 2012.[120] This would be repeating a pattern seen in other settings where the most routine tasks are initially outsourced and eventually automated.[121]

C. MACHINE COMPLEXITY VERSUS TASK COMPLEXITY

To develop a better sense of the relationship between the difficulty to automate a task and the difficulty for a human lawyer to perform the task, we show in Table 3 the distribution of hours spent on tasks in large law firms (employment = 1000+). Large law firms employ only a small fraction of all lawyers, but as with Adam Smith's pin factory, a large firm allows lawyers in different positions to specialize in different tasks (whereas a solo practitioner or small firm lawyer must perform all tasks). The economist's assumption of profit maximization suggests the law firm will assign a task to the least expensive lawyer who can perform it at an acceptable level. Thus, assignment of tasks within the large firm provides insight on how law firms rank the complexity of tasks, with the simplest tasks performed by the least experienced lawyers and the most complicated tasks performed by the most experienced ones.

TABLE 3
DISTRIBUTION OF TIME ON TASKS BY TENURE IN TIER ONE FIRMS

	Associates ≦ 2 Years	Associates >2 Years	All Partners	Tier One Total
Strong Employment Effects	**8.5%**	**4.5%**	**1.1%**	**4.1%**
Document Review	8.5%	4.5%	1.1%	4.1%
Moderate Employment Effects	**34.9%**	**38.5%**	**44.7%**	**39.0%**
Case Administration/Management	3.4%	2.4%	6.0%	3.7%
Document Drafting	4.4%	5.4%	4.8%	5.0%

[118] *See supra* note 12.

[119] *See A Less Gilded Future*, ECONOMIST (May 5, 2011), http://www.economist.com/node/18651114 [https://perma.cc/HQ37-ULHL]; Eli Wald, *Foreword: The Great Recession and the Legal Profession*, 78 FORDHAM L. REV. 2051 (2010).

[120] *See, e.g.*, Ashby Jones & Joseph Palazzolo, *What's A First-Year Lawyer Worth?*, WALL ST. J., Oct. 17, 2011 (reporting that twenty percent of corporate legal departments insist that no first- or second-year attorneys work on their matters).

[121] For example, transcription of physicians' dictated reports was first done by U.S. secretaries. It later shifted to secretarial services in the Philippines and other offshore locations. It is now largely done by automatic speech recognition.

	Associates ≦ 2 Years	**Associates >2 Years**	**All Partners**	**Tier One Total**
Due Diligence	2.0%	1.6%	2.7%	2.0%
Legal Research	1.6%	0.4%	0.1%	0.5%
Legal Analysis and Strategy	23.5%	28.7%	31.1%	28.5%
Light Employment Effects	**56.3%**	**56.6%**	**54.2%**	**56.0%**
Document Management	0.7%	0.5%	0.2%	0.4%
Fact Investigation	13.9%	9.2%	6.7%	9.2%
Legal Writing	10.1%	12.5%	9.5%	11.4%
Advising Clients	8.3%	6.2%	14.8%	9.3%
Communications and Interactions	9.0%	11.1%	5.1%	8.8%
Court Appearances	12.0%	14.7%	13.8%	13.9%
Negotiation	2.4%	2.3%	4.2%	3.0%
Totals**	99.7%	99.5%	100%	99.1%
Addendum: % of Hours Billed by Tenure	18.0%	50.0%	32.0%	100.0%

** Percentages may not sum to 100% due to rounding.

Table 3 reveals the absence of a strong association between the ease of automating a task (machine complexity) and whether the task is performed by a junior associate, a senior associate, or a partner (task complexity as viewed by the firm). Some data point toward a connection. Document review is heavily computerized, and when it is performed by firm lawyers (as opposed to contract attorneys), it is largely performed by junior associates. Advising clients is difficult to computerize and much of it is performed by partners. If these were the only two data points, they would suggest that tasks with the lowest machine complexity are assigned to the least experienced lawyers, and tasks with the highest machine complexity are assigned to the most experienced lawyers. This, in turn, would confirm the conventional wisdom that computers are having their greatest impact on the lowest level of lawyers within a firm. But the actual pattern is far less neat. The tasks of fact investigation and communication/ interactions both have minimal computer penetration, and yet junior associates spend a greater percentage of their time on both tasks than do partners.

The factor that undermines a simple relationship between machine complexity and position within a firm is unstructured human interaction, a skill that has so far resisted automation but that is a part of lawyering tasks at every level.[122] The task of advising clients may require more experience than fact investigation, but both

[122] Remus, *Reconstructing Professionalism*, *supra* note 10, at 33–34.

require an ability to conduct unstructured communication with other people—something junior associates and partners can do but computers cannot—which, in turn, illustrates that despite massive amounts of computing power, many tasks that are easy for humans are exceedingly difficult for computers.[123]

D. ESTIMATING EMPLOYMENT IMPACTS

Estimating employment impacts requires translating "Strong," "Moderate," and "Light" employment effects into percentage reductions in lawyers' hours—an exercise that is imprecise at best.[124] We nevertheless construct estimates by combining judgments based on interviews with two examples from among a limited set of studies on the effect of automation on other occupations.[125] These studies, which we describe in more detail in the Appendix, focus on computers' impacts on employee productivity (output per hour of labor). When the volume of work is assumed constant (the partial equilibrium calculation), a five percent gain in output per hour of labor results in a five percent reduction of work. We also assume that the quality of lawyers' work remains constant—that lawyers use technology to produce a constant product in less time rather than an improved product with no reduction in time. As noted above, industry surveys and data from the U.S. Bureau of Labor Statistics suggest that at present, a constant volume of work is a realistic assumption.[126] Nonetheless, given the necessary imprecision of our estimates, some readers may find the calculation unhelpful. We offer it as a step in making more tangible the frequent predictions of computers displacing lawyer labor.

Strong Employment Effects: Only one legal technology systematically falls within this category—automated document review, which was Markoff's origi-

[123] This proposition explains why automation has historically had its greatest effect on "mid-skilled" jobs, such as assembly line and clerical work. It has had much less of an effect on the lowest wage jobs because those jobs involve both unstructured human interaction and unstructured physical movement. *See* Autor et al., *supra* note 22.

[124] Among white-collar occupations, a cause of imprecision is the lack of good output measures that would allow measuring changes in employment holding output constant. Among blue-collar occupations, a cause of imprecision is the overlap between jobs that are being automated and jobs that are being sent offshore. Frank Levy & Richard J. Murnane, *How Computerized Work and Offshoring Shape Human Skill Demands*, *in* LEARNING IN THE GLOBAL ERA: INTERNATIONAL PERSPECTIVES ON GLOBALIZATION AND EDUCATION (Marcelo M. Suarez-Orozco ed., 2007).

[125] Autor et al., *supra* note 22, at 432; Sinan Aral et al., *Information, Technology and Information Worker Productivity: Task Level Evidence* (Nat'l Bureau of Econ. Research Working Paper No. 13172, 2007), http://www.nber.org/papers/w13172.pdf [https://perma.cc/EMN6-Q9QD]; Susan Athey & Scott Stern, *The Impact of Information Technology on Emergency Health Care Outcomes*, 33 RAND J. ECON. 399 (2002); Ann Bartel et al., *How Does Information Technology Affect Productivity? Plant-Level Comparisons of Product Innovation, Process Improvement, and Worker Skills*, 122 Q.J. ECON. 1721 (2007); Julia Adler-Milstein & R. Robert S. Huckman, *The Impact of Electronic Health Record Use on Physician Productivity*, 19 AM. J. MANAGED CARE 345 (2013).

[126] *See supra* note 39.

nal example.[127] Automated document review continues to require senior lawyer time to train the software and review the results, and is not efficient for small classification problems. Nonetheless, to avoid underestimating automation's employment impacts, we assume that automated document review for discovery replaces eighty-five percent of all lawyer hours currently assigned to this task.

In theory, online dispute resolution and expert systems could also fall into the category of heavy employment effects given that when used, they entirely replace lawyers (and in the case of online dispute resolution, judges as well). Their impact on lawyer employment may be significant in the future, but we estimate it is minimal at present. As discussed above, use of online dispute resolution programs is currently limited, and the disputes that these programs resolve are generally small stakes e-commerce issues for which it would not be economically feasible to hire a lawyer and litigate (such that lawyer labor is not being replaced).[128] Similarly, expert systems are generally directed at reaching new markets rather than improving efficiency in existing tasks. For example, a law firm might offer subscriptions to an expert system covering aspects of tax compliance to clients who otherwise might not consult a lawyer,[129] increasing the firm's business but not displacing any lawyers.[130]

Moderate Employment Effects: Moderate employment effects arise when a largely unstructured legal task has a significant structured component that can be computerized—for example, a computer-aided precedent search, the structured part of due diligence, or the question answering components of legal research. To calibrate the employment impact of this level of innovation, we refer to a case study of search-related innovation in exceptions processing at a large bank, discussed in the Appendix, and estimate that lawyering tasks in which computers have a Moderate Employment Effect reduce lawyer time devoted to those tasks by nineteen percent.[131]

Light Employment Effects: This category encompasses Fact Investigation, Legal Writing (as distinct from Legal Drafting), Advising Clients, Communications/Interactions, Court Appearances, and Negotiation.[132] These are tasks that entail largely unstructured work with limited room for automation.

To calibrate Light Employment Effects, we use a case study of a limited computer innovation in healthcare, discussed in the Appendix, that concluded that one standard deviation in the use of an EMR increases clinician productivity by five percent. Based on that, we posit that adopting a computer innovation with

[127] *See* Markoff, *supra* note 1.

[128] *See supra* notes 106–09 and accompanying text.

[129] *See supra* note 113 and accompanying text.

[130] The existence of markets for such systems points to the relationship between automation and proportionality, discussed below. *See infra* Part II.C.5.

[131] *See* Autor et al., *supra* note 22, at 437.

[132] Light employment effects also arise in tasks relating to document management. Because these tasks are usually performed by clerical staff, automation does not affect lawyer employment per se.

Light Employment Effects would decrease required lawyer employment for a given task by five percent.

This leaves one set of technologies for which even the roughest estimation of employment impacts is exceedingly difficult—document templates sold directly to the public by firms like LegalZoom and Rocket Lawyer. Many commentators believe these templates will fully eliminate many lawyers' jobs.[133] There is reason to question such assertions, as it is not at all clear whether these services are tapping into a latent market of previously unserved individuals or taking business away from lawyers. LegalZoom representatives argue that it is overwhelmingly the former—that they serve individuals who would not otherwise have gone to a lawyer[134]—but it is of course in their interests to frame their business model as non-threatening to lawyers.

Indirect evidence of LegalZoom's impact on market share comes from its 2012 decision to table its planned initial public offering after receiving insufficient interest from the markets.[135] Since that time, there is reason to think that LegalZoom's business has not grown as rapidly as it had projected.[136] This may be the result of regulatory responses from unauthorized practice of law committees, a topic that we address below. But regardless of cause, the slowed growth offers reason to question sweeping conclusions about massive lawyer displacement. Because of all of these uncertainties, and because any impact will be felt primarily by solo practitioners or small firm lawyers, we do not separately account for the impact of document templates marketed directly to the public. Instead we include it under the general heading of document drafting—a task with moderate computer penetration, for which relevant technologies tend to replace parts but not all of a lawyer's job.

To summarize, our illustrative calculation rests on three estimates:

- Tasks where computer technology has a strong employment effect experience an eighty-five percent reduction in employment.

[133] *See, e.g.*, McGinnis & Pearce, *supra* note 2, at 3065–66; Barton, *The Lawyer's Monopoly*, *supra* note 5, at 3068; *see also, e.g.*, BARTON, GLASS HALF FULL, *supra* note 5.

[134] Telephone Interview with Eddie Hartman, Chief Prod. Officer, LegalZoom (Sept. 18, 2015).

[135] Olivia Oran, *UPDATE 1—LegalZoom IPO Delayed—Source*, REUTERS (Aug. 2, 2012), http://www.reuters.com/article/2012/08/02/legalzoom-idUSL2E8J2EZF20120802 [https://perma.cc/RNN7-38D7]. For LegalZoom's filed Form S-1, see LegalZoom.com, Inc., Registration Statement (Form S-1) (May 10, 2012).

[136] *See, e.g.*, Michael Carney, *The $425M LegalZoom Deal Is a Win for VCs, but Less Exciting for the Company or LA*, PANDO (Jan. 6, 2014), https://pando.com/2014/01/06/the-legalzoom-deal-is-a-win-for-vcs-but-less-exciting-for-the-company-or-la/ [https://perma.cc/QDD4-W3HY] (describing a $200 million investment by private equity firm Permira as "a bit 'meh,'" and the company's $425 million valuation in the deal as "a slight downgrade from the $500 million-plus valuation . . . the company was most recently hoping to attract in the public markets [as part of the proposed IPO]"); *Has LegalZoom Lost its Bloom?*, THEFORMTOOL (Jan. 6, 2013), http://www.theformtool.com/has-legalzoom-los-its-bloom/ [https://perma.cc/8N5X-H3FG] (describing that prior to the proposed IPO, "LegalZoom was already experiencing the chill of a slowing growth rate and tighter margins in its traditional market, legal forms for sale.").

- Tasks where computer technology has a moderate employment effect experience a nineteen percent reduction in employment.
- Tasks where computer technology has a light employment effect experience a five percent reduction in employment.

To calculate an overall employment impact, we apply these percentages to the lawyers' use of time in 2014 in Tier 1 firms (Table 3).[137] Table 3 reflects our use of a partial equilibrium calculation, which makes our argument transparent but requires two strong assumptions: (i) that no employment impacts from these technologies have occurred previously, and (ii) that the level of work remains constant. If all the technology above were implemented at one time, it would result in an estimated thirteen percent reduction in hours.[138] Since law firms have a well-established reputation for slow technology adoption, however, we assume more realistically that the technology is adopted over a period of five years.[139] Again, assuming a constant volume of legal work, our estimated employment loss spread over five years would indicate that demand for lawyers' hours is decreasing by 2.5 percent per year because lawyer productivity is increasing by 2.5 percent per year.[140] In considering this estimate, we note that labor productivity increasing by 2.5 percent per year is an impressive number; labor productivity across the U.S. non-farm business sector has averaged slightly less than 1.5 percent growth per year for the last ten years.[141]

To summarize, it is frequently argued in popular writing on artificial intelligence that the automation of legal work causes weakness in the market for lawyers. Our estimates indicate that the argument is overstated and that a more important cause is a basic imbalance between supply and demand. Interviews suggest that by 2004, significant numbers of contract lawyers could be hired, at a much cheaper rate than law firm associates, to classify the huge volume of digital documents that had become part of discovery proceedings. In 2009, National Law Journal (NLJ) 250 firms laid off 5,259 attorneys—about four percent of all

[137] Recall that the distribution of time on task in Tier 2–Tier 5 firms is similar to the distribution in Tier 1 firms.

[138] Our job loss estimate will be low if solo practitioners spend much of their time on non-adversarial, formulaic issues that could be replaced by templates sold directly to individuals. We may also be underestimating predictive coding's impact on contract lawyer employment, but interviews with industry professionals and corporate counsels in charge of discovery suggest this is not the case. They argue that predictive coding has replaced contract lawyers in some, but not all, parts of the discovery document classification while the volume of discovery work has grown enough to maintain employment levels.

[139] The slow adoption of legal technology was emphasized in many of our interviews. We explain why adoption may start growing more rapidly in Part II.

[140] Alternatively, the volume of legal services would have to increase by at least 2.5 percent per year to offset automation's impact in reducing demand for lawyers' services.

[141] *See, e.g.*, EXEC. OFFICE OF THE PRESIDENT COUNCIL OF ECON. ADVISERS, ECONOMIC REPORT OF THE PRESIDENT app. B, tbl.B-16 (2015).

NLJ 250 attorneys (including 8.7% of NLJ 250 associates).[142] If we consider the beginning of the legal artificial intelligence age the 2012 *Da Silva Moore* decision affirming technology-assisted review, then we can say computerized work has been one of many drags on a generally weak market.

Our calculations rested on a number of assumptions, however, which admittedly narrow the inquiry and simplify reality. In the next part, as we look ahead to future developments, we broaden our focus. We acknowledge that the demand for legal work will not stay constant as new technologies are adopted, that technology may improve the quality as opposed to efficiency of legal work, and that professional regulation will play a key role in steering the direction of technological advances.

II. LEGAL PROFESSIONALISM IN THE DIGITAL AGE

Part I offered estimates of current employment impacts of existing and emerging legal technologies. In this Part, through a series of three questions, we broaden our focus to consider the direction of longer-term technological development and the role of regulation in conditioning that development. First, we ask how legal technologies—specifically, artificial intelligence applications that potentially perform work now performed by lawyers[143]—would likely develop and expand if market forces operate freely. Of course, the market for legal services does not operate freely; it is highly regulated, with significant repercussions for the development of legal technologies. We therefore also examine existing regulatory structures, showing that they are inadequate to address the challenges and opportunities of new technologies. Third and finally, we argue that notwithstanding deep problems with existing approaches to regulation, unimpeded market forces will have deleterious effects while professional norms and regulations have continuing value. We conclude by addressing the challenge of designing regulatory structures that protect professional values without excessively impeding the development and adoption of, and access to, new legal technologies.

A. THE MARKET FOR NEW TECHNOLOGIES

The likely path for legal artificial intelligence will be shaped by two propositions discussed in Part I:

- For a computer to automate a lawyer's task, it must be possible to model the lawyer's information processing in a set of instructions; and

[142] Leigh Jones, *So Long, Farewell; There's No Sugar Coating It: This Was the Worst Year Ever for Lawyer Headcount*, NAT'L L.J., Nov. 9, 2009.

[143] Law firms also will be involved with other software—in particular, data security and cloud applications—that do not have obvious implications for employment.

- Models estimated by machine learning have difficulty processing contingencies that differ significantly from the data on which the models were trained.

The first proposition limits legal applications to structured tasks—tasks for which information processing follows an underlying pattern (which may be uncovered by machine learning). The second proposition encourages developers to focus the machine learning on relatively narrow tasks—tasks where it is feasible to train the model on most of the contingencies it is likely to confront (though this training may occur over time as the model is used).[144]

These restrictions are apparent in the progress of legal artificial intelligence to date: major inroads in document classification in discovery (the subject of Markoff's original article[145]) and developing inroads in organizing, drafting, and reviewing contracts for due diligence. Other applications are at more embryonic stages: question answering systems using highly trained databases; improved search and information extraction tools to locate particular information within the enterprise or within a particular body of documents; data-based tools for cost and risk analysis and prediction; and expert systems that offer a platform to provide pre-packaged legal advice.

With the exception of expert systems, these applications all involve language processing—in particular, measuring the similarity of meaning between two documents (or pieces of text). By focusing on comparisons between two documents, the software sidesteps problems in inferring meaning in less structured situations—for example, interpreting a client letter that uses common sense reasoning as part of its language.[146] The difficulty in solving these problems helps to explain why artificial intelligence has not, to this point, penetrated those lawyers' tasks that require unstructured communication.

Despite these limitations, artificial intelligence will both extend existing applications and address other structured tasks. An example of an extension begins with Vern Walker's argument, noted earlier, that an ultimate goal of legal search tools is to locate legal arguments rather than entire cases or text passages.[147] Currently, the advanced applications in this area, such as IBM's Debater System, are based on a document corpus where claims and evidence have been annotated by humans. Improvements in natural language processing

[144] Absent from this description is the human ability to draw correct inferences from small amounts of information, a key element in the flexibility of human cognition.

[145] *See* Markoff, *supra* note 1.

[146] Common sense refers to the large set of facts that people apply without thinking but computers don't recognize unless they are programmed to do so—for example, a screwdriver dropped from the hand falls down rather than up or sideways. *See* Ernest Davis, *How to Write Science Questions that Are Easy for People and Hard for Computers*, AI MAG., Spring 2016, at 13.

[147] *See supra* note 76 and accompanying text.

are making some progress in identifying claims and evidence automatically.[148]

Similarly, several applications now offer advanced proof reading of documents including identifying inconsistent use of terms, improper citation formats, and other features beyond basic spelling and punctuation.[149] As with predictive coding and contract review, these applications have the potential to save lawyer time. One exception to this trend is the much-discussed development of blockchain-based contracts,[150] which appear, at least for now, to be confined to heavily repeated trades of financial instruments where the work involved was previously performed by back office personnel rather than lawyers.[151]

Improved applications are one way to increase the reach of legal artificial intelligence. An alternative approach is to simplify the task so that computers can perform currently complex tasks with existing software. Kingsley Martin, a developer of contract review software, envisions the development of "auditable contracts"—contracts written in English that are simple enough to be parsed by a computer.[152] Such contracts could, in theory, substantially improve automated contract review. As another example, Modria, the online dispute resolution program, simplifies the task of negotiation by gathering information from each side, summarizing areas of agreement and disagreement, and, based on that information, presenting proposed resolutions.[153] The program also has mediation and arbitration modules if the parties cannot agree to one of the proposed resolutions, but the company claims that the "vast majority" of claims are settled just by laying out the facts and proposing solutions based on areas of agreement.[154]

In some cases, a task can be simplified or standardized without altering its meaning. For example, an individual orders a book from Amazon by clicking on an icon rather than writing a free text email (with potential mistakes), which would be hard to automatically interpret. In other cases, however, part of a task will be lost in the simplification. Recall that early versions of Westlaw and Lexis

[148] Ruty Rinott et al., *Show Me Your Evidence—An Automatic Method for Context Dependent Evidence Detection*, at 440 (Ass'n for Computational Linguistics, Proc. of the 2015 Conf. on Empirical Methods in Nat. Language Processing, Sept. 2015), http://aclweb.org/anthology/D15-1050?cm_mc_uid=73807758537314226464001&cm_mc_sid_50200000=1473173993 [https://perma.cc/YV4T-K3EZ].

[149] *See, e.g.*, *Contract Companion*, MICROSYSTEMS, http://www.microsystems.com/contractcompanion [https://perma.cc/47LR-LZYB] (last visited Apr. 2, 2017).

[150] A blockchain contract rests on a computer protocol that specifies the terms of an agreement—payments to be made when specified conditions are satisfied and so on. By embedding the protocol in a blockchain—a distributed ledger—the contract is protected from manipulation by either party and the parties do not need a bank or other trusted intermediary to enforce contract terms. As noted earlier, to be written as a computer protocol, a contract must involve only well-defined elements.

[151] *See, e.g.*, Atsushi Santo et al., *Applicability of Distributed Ledger Technology to Capital Market Infrastructure*, at 5–6 (Japan Exch. Grp., Working Paper Vol. 15, 2016), http://www.jpx.co.jp/english/corporate/research-study/working-paper/b5b4pj000000i468-att/E_JPX_working_paper_No15.pdf [https://perma.cc/9E32-WT5H].

[152] Telephone Interview with Kingsley Martin (Aug. 2017).

[153] *See* MODRIA, http://modria.com/ [https://perma.cc/9EKG-S5JD] (last visited Mar. 2, 2017).

[154] *Id.*

simplified the task of searching for legal concepts and arguments by allowing users to look for particular words or combinations of words. Simplifying the search task to a keyword search distorted the results, leading Westlaw and Lexis to reintroduce broader approaches to legal research, such as through headnotes and indexes.

In addition to impacting technology development, the market will of course influence adoption. Historically, law firms have resisted new technologies of most kinds, but for reasons that now might be changing. As long as clients were willing to pay on the basis of billable hours, the need for technology to increase efficiency was not an imperative. The partnership structure of many law firms further increased resistance because technology costs come directly from partners' profits.[155] A third source of resistance was the well-documented distaste that many lawyers have for technology and "mathiness" of any kind.[156]

While much of the legal services market continues to use billable hours, client pressure on hourly rates and total hours is likely to continue to intensify, reflecting the continuing imbalance between the supply of lawyers and the demand for legal services. In Am Law 100 and 200 firms surveyed by the Thomson Reuters *Peer Monitor*, total billable hours have shown virtually no growth since 2010, while the number of lawyers across all U.S. law firms has grown by one to two percent per year.[157] As pressure increases to hold down expenses, the purchase of technology becomes more attractive.

A second factor promoting accelerated technology purchases is the shift of corporate legal work from law firms to the corporation's own legal department. Such legal departments are part of standard, profit-maximizing organizations that put a higher value on efficiency than a partner-based firm.[158]

A third but more speculative factor promoting accelerated technology adoption may be Clay Christensen's theory of disruptive innovation.[159] Initially, Big Law

[155] We thank Bruce Elvin for this point. In a traditional corporation, the cost of technology is borne by shareholders.

[156] *See, e.g.*, Susan Moon, *Moonlighting: Things Not to Say In-House—'I'm Bad at Math'*, ABOVETHELAW (Jan. 6, 2012), http://abovethelaw.com/2012/01/moonlighting-things-not-to-say-in-house-im-bad-at-math/ [https://perma.cc/V6R5-RAAN].

[157] *See* 2016 LEGAL MARKET REPORT, *supra* note 39, at 4, chart 3.

[158] *See, e.g.*, Deborah A. DeMott, *The Discrete Roles of General Counsel*, 74 FORDHAM L. REV. 955, 958–60 (2005); Robert L. Nelson & Laura B. Nielsen, *Cops, Counsel, and Entrepreneurs: Constructing the Role of Inside Counsel in Large Corporations*, 34 LAW & SOC'Y REV. 457, 466–68 (2000).

[159] "Disruptive Innovation" is Clayton Christensen's theory of the impact of technological innovation on markets. CLAYTON M. CHRISTENSEN, THE INNOVATOR'S DILEMMA (2013). Christensen argues that companies (here, law firms) at the top of the market routinely ignore disruptive technologies in their early days because such technologies focus on the bottom of the market and do not constitute competition. Such companies may even abandon low margin work to these new technologies so as to focus on higher margin work. But the technology producers and vendors that initially targeted the lower end of the market eventually improve their products and services to address higher margin work. Eventually, what appeared to be the best short-term strategy for firms at the top of the market (ignore the new technologies) turns out to enable competition and displacement.

did not appear at all concerned about losing routine work to insourcing, outsourcing, or automation, because it was work for which clients were already (and from firms' perspective, problematically) demanding lowered fees and alternative fee arrangements.[160] But accepting and performing the routine work allowed software developers and legal technology firms to develop approaches and solutions to more complicated and profitable work, which Big Law may have little choice but to adopt under client pressure. Ben Barton and others have predicted that this pattern may repeat on a more dramatic scale with online legal service providers like LegalZoom and Rocket Law, first displacing solo practitioners and small firms, and gradually disrupting the entire law firm model.[161] Regardless of whether Christensen's theory plays out in full, it seems likely that technology solutions at the bottom of the market will push change throughout the market.

All of this said, the implications of an acceleration in technology adoption for legal employment are not clear. As we have seen, some kinds of software may primarily address new markets—LegalZoom, for example. Other kinds of software represent new kinds of service that may expand rather than reduce the need for lawyers—for example, expert systems and prediction analytics to measure risk. In addition, the context of the work matters. When applied to pro forma activities—legal tasks that can be completed by applying a fixed amount of effort to anticipated contingencies—artificial intelligence substituting for a lawyer's time will likely reduce the demand for lawyers. Examples include incorporating a new business, writing a will, or ensuring internal compliance with a particular statutory scheme. In adversarial activities, in contrast, a party's effort is generally determined in part by the efforts of the other party, where the other party has strong incentives to develop *unanticipated* contingencies. Here, it is possible that the two parties settle into an arms race in which they use the time that artificial intelligence frees up for other activities.

Accordingly, the likely trajectory of legal technologies in an unregulated market would be determined by factors affecting both development and adoption. We believe the pace of development would depend largely on advances in natural language processing while the pace of adoption would depend on client pressures.

B. CURRENT APPROACHES TO REGULATION

Of course, the market for legal services is far from unregulated. Unauthorized Practice of Law (UPL) rules limit the provision of legal services to individuals

[160] *See, e.g.*, *Events: Disruptive Innovation in the Market for Legal Services*, HARV. LAW SCH. CTR. ON THE LEGAL PROF. (Mar. 6, 2014), https://clp.law.harvard.edu/event-post/disruptive-innovation-in-the-market-for-legal-services/ [https://perma.cc/2QZY-GHMQ].

[161] Barton acknowledges, however, that bespoke "bet the company" work will remain an exclusive domain of law firms.

who are trained and licensed to practice law.[162] State supreme courts and bar committees then discipline lawyers who fail to adhere to the rules of practice and ethical codes. We see a continuing need for, and value in, professional regulation. However, for at least four reasons, the UPL rules—the principal way in which the profession currently addresses new technologies—provide an unhelpful approach.

First, courts following this approach have posed for themselves an unanswerable question. UPL rules seek to distinguish tasks that can only be performed by trained and licensed lawyers from tasks that lay people, lacking the same training and ethical regulation, can nevertheless provide competently, reliably, and ethically. Courts have applied this framework to new technologies by asking whether a given technology (generally an online service provider) is more similar to a scrivener who completes a form by merely recording the information a customer relays (in which case, the technology would not constitute UPL) or to a service provider who aids in selecting and properly completing a form (in which case, it would constitute UPL).[163] Neither alternative is ever clearly right or wrong.[164] An online legal forms provider can be viewed as the functional equivalent of a mere scrivener insofar as it is the user him or herself who enters the relevant information via the online questionnaire and completes the form;[165] or the provider can be viewed as the functional equivalent of a human service provider exercising judgment insofar as the software is programmed with deductive rules to ask the user a series of questions and, based on the answers, complete the appropriate document.[166] Accordingly, courts are left making normative decisions with little guidance from the framework.

Second, analogizing to human approaches fails to appreciate that which is unique and distinct about legal technologies. Computers can be trained in ways that avoid human error such that we may be comfortable with a computer performing tasks we would not want performed by an untrained and potentially

[162] The principal justification prohibiting unauthorized practice of law is "to protect the public from the consequences of receiving legal services from unqualified persons." ANNOTATED MODEL RULES OF PROF'L CONDUCT R. 5.5 (2015) [hereinafter ANN. MODEL RULES] (Rationale for Proscription Against Unauthorized Practice of Law) ("The proscriptions are also aimed at facilitating the regulation of the legal profession and protecting the integrity of the judicial system.").

[163] *See, e.g.*, Janson v. LegalZoom.com, Inc., 802 F. Supp. 2d 1053, 1059 (W.D. Mo. 2011) ("Plaintiffs urge the Court to follow the cases . . . which generally involve businesses providing a legal document preparation service for their customers. . . . Defendant LegalZoom argues that its website providing access to online document assembly software is the functional equivalent of [a] 'do-it-yourself' divorce kit . . . .").

[164] The court in *Janson* even acknowledged this, but declined to revise its analysis accordingly. *See id.* at 1063 ("None of the . . . cases cited by the parties are directly on point, due to the novelty of the technology at issue here.").

[165] *See id.* (noting LegalZoom's argument that "its customers—rather than LegalZoom itself—complete the standardized legal documents by entering their information via the online questionnaire to fill the document's blanks").

[166] *See id.* at 1055 (observing that LegalZoom reassures consumers that "we'll prepare your legal documents," and that "LegalZoom takes over" once customers "answer a few simple online questions").

unreliable human.[167] And yet, reducing a lawyering task to a set of computer-implementable rules may over-simplify, ignore complexity, or create opportunities for error that are not immediately apparent.[168] We therefore may not want a computer performing particular tasks in all contexts, notwithstanding effective performance in one context.

A third problem stems from the poor fit between the UPL inquiry and technologies that lawyers use in representing clients (as opposed to those that are marketed directly to the public). Concluding that a non-lawyer cannot competently and reliably perform a particular task does not establish that a computer cannot help a lawyer do so. Perhaps for this reason, some commentators suggest that technologies that lawyers use and oversee are best addressed through the rules of lawyer oversight of non-lawyer service providers.[169] Applied to new technologies, these rules would permit adoption of new technologies where lawyers supervise their use and accept responsibility for their results. At least for now, however, few lawyers are sufficiently knowledgeable to oversee new legal technologies in a meaningful way.[170] Moreover, this approach suggests that computerizing all of a lawyer's functions would be permissible with oversight. But surely some tasks, such as in-court advocacy and settlement or plea negotiations, cannot and should not be delegated to a computer.

A fourth and final problem is that UPL prosecutions often appear to be self-interested efforts by the bar to protect its monopoly.[171] Scholars and commentators have long argued that non-lawyers can perform certain aspects of

[167] The *Janson* court ignored this, resting entirely on a formalistic UPL analysis. *Id.* at 1064 ("Because those that provide [LegalZoom's] service are not authorized to practice law in Missouri, there is a clear risk of the public being served in legal matters by 'incompetent or unreliable persons.'").

[168] *See, e.g.*, *supra* note 77 and accompanying text.

[169] These rules, developed to address the outsourcing of work to non-lawyers or offshoring of work to foreign lawyers, provide that such activities are ethically permissible so long as the lawyer supervises the work and retains ultimate responsibility for the result. *See, e.g.*, ABA Comm'n on Ethics & Prof'l Responsibility, Formal Op. 08-451 (2008) ("A lawyer may outsource legal or nonlegal support services provided the lawyer remains ultimately responsible for rendering competent legal services to the client under Model Rule 1.1."); *see also* Prof'l Ethics of the Fla. Bar, Op. 07-2 (2008) (approving of off-shore outsourcing); Ass'n of the Bar of the City of N.Y. Comm. on Prof'l & Judicial Ethics, Formal Op. 2006-3 (2006) (providing that a lawyer may outsource legal support services to overseas lawyers and non-lawyers if the lawyer supervises the work rigorously).

[170] A comment to Model Rule 1.1 advises lawyers of a professional duty to stay abreast of technological advances, *see* MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 5 (2016) [hereinafter MODEL RULES], but this provision has little teeth given the vagueness of its standard and its location in the comments rather than in an enforceable rule. Moreover, lawyers' generally low level of technical competency is reinforced by other provisions of the *Model Rules*, which prescribe a reduced level of required oversight for automated legal work. *See, e.g.*, MODEL RULES R. 5.3 cmt. 4.

[171] *See, e.g.*, DEBORAH L. RHODE, THE TROUBLE WITH LAWYERS ch. 5 (2015); Benjamin H. Barton, *Why Do We Regulate Lawyers?: An Economic Analysis of the Justifications for Entry and Conduct Regulation*, 33 ARIZ. ST. L.J. 429, 457 (2001) [hereinafter Barton, *Why Regulate Lawyers?*]; Roger C. Cramton, *Delivery of Legal Services to Ordinary Americans*, 44 CASE W. RES. L. REV. 531, 615 (1994); Deborah Rhode, *Access to Justice: Connecting Principles to Practice*, 17 GEO. J. LEGAL ETHICS 369, 371–72, 409 (2004) [hereinafter Rhode, *Access to Justice*]; Deborah L. Rhode, *Professionalism in Perspective: Alternative Approaches to Nonlawyer*

legal practice perfectly well, and that allowing them to do so would dramatically reduce the cost of legal services.[172] This argument applies to technologies as well—if technologies can, in fact, perform aspects of legal practice as well as humans, shouldn't we use them to increase access to justice? And indeed, many courts and legal services organizations are relying on technology to expand their reach. Thus far, they have done so primarily through online filing or intake systems, which simply leverage the power and reach of the Internet.[173] Commentators advocate more advanced technologies, from automated document assembly to phone apps that give legal advice, as the only workable solution to the access to justice gap.[174]

And yet, at least one formulation of this argument, recently adopted by the U.S. Court of Appeals for the Second Circuit, is highly problematic. In a case construing the exemption from over-time pay for individuals "employed in a bona fide . . . professional capacity" under the Fair Labor Standards Act,[175] the plaintiff, a contract attorney, argued that document review, defined as "us[ing] criteria developed by others to simply sort documents into different categories," did not constitute the practice of law, such that he was not employed in a "professional capacity."[176] The Second Circuit agreed, reasoning that because these were "services that a machine could have provided," they could not possibly constitute the practice of law.[177]

The Second Circuit's conclusion was based on a high-level generalization that computers can perform document review as well as humans. But neither the Second Circuit, nor scholars and commentators expressing similar reasoning, have undertaken the critical inquiry of whether and how a machine approaches the task differently from a human. The differences have ramifications that extend beyond lowered costs and are central to a meaningful normative and regulatory

Practice, 22 N.Y.U. REV. L. & SOC. CHANGE 701, 709–13 (1996) [hereinafter Rhode, *Professionalism in Perspective*].

[172] *See, e.g.*, Barton, *Why Regulate Lawyers?*, supra note 171, at 457; Cramton, *supra* note 171, at 615; Rhode, *Access to Justice*, *supra* note 171, at 371–72, 409; Rhode, *Professionalism in Perspective*, *supra* note 171, at 709–13; Laurel A. Rigertas, *Stratification of the Legal Profession: A Debate in Need of a Public Forum*, 2012 J. PROF. LAW. 79; Cristina L. Underwood, *Balancing Consumer Interests in a Digital Age: A New Approach to Regulating the Unauthorized Practice of Law*, 79 WASH. L. REV. 437, 442 (2004).

[173] *See, e.g.*, LAWHELP.ORG, http://lawhelp.org [https://perma.cc/R79Z-MF4Z] (last visited Mar. 9, 2017).

[174] *See, e.g.*, McGinnis & Pearce, *supra* note 2, at 3066; BARTON, GLASS HALF FULL, *supra* note 5; Barton, *The Lawyer's Monopoly*, *supra* note 5, at 3068; Rostain et al., *Thinking Like a Lawyer*, *supra* note 97.

[175] Lola v. Skadden, Arps, Slate, Meagher & Flom LLP, No. 14-3845-cv, 2015 WL 4476828, at *2 (2d Cir. July 23, 2015) (reviewing an appeal from an order dismissing plaintiff's putative class action for violation of the Fair Labor Standards Act, 29 U.S.C. 201 et seq., for failing to pay overtime for document review).

[176] *Id.* at *6.

[177] *Id.* Plaintiff alleged that his work was closely supervised by the Defendants, and his "entire responsibility . . . consisted of (a) looking at documents to see what search terms, if any, appeared in the documents, (b) marking those documents into the categories predetermined by Defendants, and (c) at times drawing black boxes to redact portions of certain documents based on specific protocols that Defendants provided." *Id.* at *1 (internal quotations omitted).

inquiry.[178] The computer's altered approach is often what makes automation attractive—it may sidestep opportunities for human error, improving accuracy and consistency. But it may also create new opportunities for error or have unintended consequences for legal practice. Access to deeply flawed and error-filled legal services cannot qualify as an acceptable, much less desirable, answer to the access to justice gap.

Accordingly, while we agree with the majority of critics and commentators who view the UPL rules as unreasonably impeding the pace of technological development and use, we do not think the answer is to jump to conclusions based on particular instances of a computer performing a task well. Nor, as we discuss next, do we think the answer is to forego all forms of professional regulation.

C. THE VALUE OF REGULATION

Critics contend that the problem is not only the UPL rules, but also all forms of professional regulation. Professional regulation, they contend, is an exercise in protectionism, limiting competition from computers and human service providers alike.[179] Although this critique is important and powerful, it paints only a partial picture. It fails to consider at least three essential functions of professional regulation, which are implicated by new technologies: (1) protecting consumers in the face of information asymmetries;[180] (2) ensuring that negative externalities do not undermine the integrity of our legal systems; and (3) ensuring universal access to legal services.[181] We believe that the values, norms, and structures of the legal profession are necessary to address the challenges new legal technologies pose for all three of these objectives.

[178] It is far from established that all legal technologies will lead to lowered costs. *See* Remus, *Predictive Coding*, *supra* note 47, at 1707.

[179] MILTON FRIEDMAN, CAPITALISM AND FREEDOM 139 (1962) (arguing that the state-granted power of licensure, which takes the form of monopolistic market power and the right of self-regulation, allows licensees to advance their financial self-interest at the expense of the public interest); *see also* ABBOTT, *supra* note 10, at 184–86; ABEL, *supra* note 10, at 40–48; SUSSKIND & SUSSKIND, *supra* note 2, at 16–17; Gillian K. Hadfield, *The Cost of Law: Promoting Access to Justice Through the (Un)Corporate Practice of Law*, 38 INT'L REV. L. & ECON. 43, 43 (2014); Barton, *Why Regulate Lawyers?*, *supra* note 171, at 457; Rhode, *Access to Justice*, *supra* note 171, at 371–72, 409.

[180] A primary and long-standing justification of professional regulation proceeds as follows: Because of the esoteric and specialized nature of legal expertise, lay people cannot adequately assess or monitor the work of lawyers. Professional licensure is therefore needed to ensure that those who provide legal services have a baseline level of competency; professional regulation is needed to ensure that if clients are harmed there are repercussions.

[181] An additional justification of professional regulation addresses the ways in which clients, intentionally or not, may use lawyers to the detriment of opponents or third parties. Thus, for example, the ethical rules prohibit lawyers from aiding clients who choose to perjure themselves and in some limited circumstances allow lawyers to breach a client's confidences to protect third parties.

1. CONSUMER PROTECTION

A common refrain among legal technology advocates is that by eliminating human error, standardizing services, and lowering prices, new technologies have the potential to serve client interests far more effectively than lawyers.[182] This may be true in some contexts, but it is decidedly not true in others. Moreover, many clients and lawyers alike lack sufficient understanding of new legal technologies to determine when use is appropriate and when the risk of harm or error is low or high.

Document classification offers a useful illustration of how a legal technology that eliminates error in some contexts may simultaneously create new risks of error in other contexts. A human lawyer engaging in this task examines a set of documents page-by-page to identify relevant meaning and content. Predictive coding, in contrast, identifies particular combinations of document features pursuant to statistical probabilities of relevance, with no reference to meaning. This is not a problem when the goal is to locate types of data and information that have been well specified in advance, such as in discovery practice.[183] But as we have seen, machine learning models (which are estimated statistical models) have difficulty processing contingencies that differ significantly from their training data. They therefore have difficulty processing and recognizing the unstructured aspects of due diligence that precede a corporate transaction.[184] As noted above, some firms are making progress in automating tasks encompassed by due diligence, but at least for the time being, their products are effective only in reviewing large volumes of similar documents or identifying similar types of clauses.

Even within discovery practice, predictive coding may create new risks of error by failing to recognize "hot documents"—documents that are highly relevant and damaging to the producing party. Individuals often change their normal writing styles, becoming particularly formalistic or vague, when they explain major decisions or acquire potential liability. As a result, hot documents, which document these decisions or events, frequently employ unusual or coded language or syntax. The most relevant documents in a case may therefore use language and tone that many predictive coding products, trained on a sample of normal documents, will fail to recognize.[185] Some products correct for this problem by training the computer on a sample of responsive documents rather

[182] *See, e.g.*, McGinnis & Pearce, *supra* note 2, at 3054–55; Cabral et al., *supra* note 11, at 246–56; Hornsby, *supra* note 11, at 931–34; Staudt, *supra* note 11, at 1128–34; Wolf, *supra* note 11, at 773–85.

[183] *See, e.g.*, Grossman & Cormack, *supra* note 61, at 3; Roitblat et al., *supra* note 61, at 70, 74–75.

[184] *See supra* notes 68–69 and accompanying text.

[185] Hofman Interview, *supra* note 68. Note that for some predictive coding products, the problem may be virtually intractable if the author reverts to coded language (i.e., "I bought two pounds of flounder at the fish market today" to indicate a completed transaction). *Id.*

than random documents[186] and/or by identifying responsiveness by reference to metadata as well as words.[187] But the user must be able to understand and to recognize the importance of selecting the best and most appropriate product. Otherwise, the machine-learning algorithm may fail to recognize a hot document, and, because it will not recognize the existence of a problem in these situations, it will not give the user a warning.

This is one example of the broader challenge posed by machine learning models—the task of determining when and how to notify a user that the computer's "best" answer is not very good. Some predictive coding applications deal with this problem forthrightly by assigning each document an ex ante probability of responsiveness.[188] In a similar approach, software that compares documents can calculate a mathematical index of similarity and a user can specify a cutoff below which documents are judged as not sufficiently similar. But in other cases, the user is at the mercy of the programmer. On different dates, an iPhone "Siri" responded to the question, "Can a dog jump over a house?" with "I'm sorry but I don't know the answer to that question"[189] or by offering a link to a child's riddle about a dog jumping over a doghouse and a second link to an ASPCA bulletin on teaching dogs not to jump.[190]

Our point is not that predictive coding has no value or should never be used, nor is it that unanticipated contingencies represent insurmountable hurdles to automation. We mean only to emphasize that consumer protection concerns are as salient with respect to legal technologies as they are with respect to legal services generally. In both cases, the expertise in question is complex, esoteric, and specialized; in both cases information asymmetries can quickly lead to market failure.

And yet, the answer cannot be traditional forms of professional regulation, as lawyers themselves frequently lack sufficient understanding of the technologies. As discussed, predictive coding increases the risk for error, in some cases at the same time that it decreases the risk in others, but understanding how and why, and choosing the most appropriate tool and protocol for the context, requires

[186] *See* Grossman & Cormack, *supra* note 61 ("Random training tends to be biased in favor of commonly occurring types of relevant documents, at the expense of rare types. Nonrandom training can counter this bias by uncovering relevant examples of rare types of documents that would be unlikely to appear in a random sample.").

[187] Grossman & Cormack Interview, *supra* note 57. For example, a tool that identifies responsiveness exclusively by reference to words may not identify an email written in coded language, but a tool that also references metadata may identify it by focusing on who is emailing whom and when, and not just on the content of the message.

[188] These probabilities are examples of the developing area of "explainable artificial intelligence." *See* Marco Tulio Ribeiro et al., *"Why Should I Trust You?": Explaining the Predictions of Any Classifier*, ACM SIG KDD INT'L CONF. ON KNOWLEDGE DISCOVERY & DATA MINING (KDD) (Aug. 9, 2016).

[189] Question posed on Aug. 14, 2015.

[190] Question posed on Nov. 27, 2015.

significant technological expertise that many lawyers lack. As we return to below, effective regulation may therefore require technical as well as legal expertise.

2. SYSTEMIC INTERESTS

The value of professional regulation lies not only in protecting clients from lawyers (or legal technologies), but also in protecting society from the ways in which clients may use lawyers (or legal technologies) to the detriment of others, including opponents, third parties, and the legal system itself. Some degree of this is built into our adversarial system—clients hire lawyers precisely in order to gain an advantage over others. But codes of conduct place limits on what lawyers can do for their clients. They ensure, for example, a baseline of fair dealing with an opponent, candor to the court, and respect for the rule of law.[191]

New legal technologies implicate these interests in important but non-obvious ways. For example, clients may be eager to use, or to have their lawyers use, legal prediction software, given that it often achieves higher levels of accuracy than human prediction.[192] But if such software completely displaces lawyers, the increased accuracy may be accompanied by a number of detrimental consequences. Reducing advice to prediction would eliminate a core function of lawyering—counseling compliance with the law. If a client's only legal advice comes from a computer's prediction of how a court will likely respond, advising will be reduced to calculating what a client can get away with, instantiating the Holmesian Bad Man view of the lawyer.[193]

More broadly, reducing legal advising to legal prediction could threaten to impede the law's development. Predictability and stability are of course critical rule-of-law values, but so too is democratic participation in lawmaking.[194] A core

[191] *See, e.g.*, MODEL RULES R. 4.1, 8.4(c); RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 98(1) cmt. b (2000).

[192] *See* Theodore W. Ruger et al., *The Supreme Court Forecasting Project: Legal and Political Science Approaches to Predicting Supreme Court Decisionmaking*, 104 COLUM. L. REV. 1150, 1152 (2004) (reporting that a statistical model, which relied on general case characteristics predicted seventy-five percent of the Court's affirm/reverse results correctly, while legal experts collectively got 59.1 percent right); *see also* Elizabeth Earl, *Law Profs Develop Supreme Court Predictor to Better Understand Court Decisions*, A.B.A. J. (Dec. 1, 2014), http://www.abajournal.com/magazine/article/law_profs_develop_supreme_court_predictor/?utm_source=maestro&utm_medium=email&utm_campaign=tech_monthly [https://perma.cc/U3U9-RN8J]. Evidence suggests more broadly that statistical prediction is more accurate than clinical prediction in most contexts. *See* William M. Grove, *Clinical Versus Statistical Prediction: The Contribution of Paul E. Meehl*, 61 J. CLINICAL PSYCH. 1233 (2005).

[193] *See* Oliver Wendell Holmes, *The Path of the Law*, 10 HARV. L. REV. 457 (1897); Robert Cooter, *Do Good Laws Make Good Citizens? An Economic Analysis of Internalized Norms*, 86 VA. L. REV. 1577, 1591 (2000) ("[T]he 'bad man' treats the law as 'external' to himself, in the sense that he considers it to lie outside of his own values. Economic models of law typically accept the 'bad man' approach and add a rationality element to it: a rational 'bad man' decides whether or not to obey the law by calculating his own benefits and costs, including the risk of punishment.").

[194] Jeremy Waldron, *The Concept and the Rule of Law*, 43 GA. L. REV. 1, 5 (2008) ("[O]ur understanding of the Rule of Law should emphasize not only the value of settled, determinate rules and the predictability that

way in which citizens participate is through their lawyers, who translate their interests into persuasive and sometimes novel arguments as to how the law should apply to their clients' circumstances. Lawyers can do so because our legal system is about reasons as well as outcomes—reasons, asserted by lawyers and memorialized in judicial opinions, which provide a continual opportunity through which to debate and potentially change the law.[195] If lawyering is replaced by computer prediction, we will shift to a system that is more about outcomes than reasons—and outcomes that are inescapably "informed by the world as it was in the past, or, at best, as it currently is."[196]

Of course, this may change over time. As natural language processing capabilities advance and computers become more capable of processing concepts and analogies, combinatorial processing may join computer prediction with computer creativity. As lawyers recognize, creativity and novelty in legal arguments generally come from importing legal concepts from one area of law into another, and by combining existing arguments in new and persuasive ways. Indeed, knowledge production in many fields proceeds in this way—by recombining existing ideas in new and innovative ways.[197] Computers cannot currently do this, but their ability to do so will likely increase over time. Much as medical diagnostic programs currently suggest disease hypotheses to physicians based on patient symptoms,[198] legal argument programs may soon be able to suggest new and promising combinations of existing arguments tailored to a client's factual circumstances. For now, computer programs are highly effective in making predictions given the legal system as it currently exists, but far less so in making suggestions for how the legal system could or should evolve.

such rules make possible, but also the importance of the procedural and argumentative aspects of legal practice."); *see also* Benjamin Ewing & Douglas A. Kysar, *Prods and Pleas: Limited Government in an Era of Unlimited Harm*, 121 YALE L.J. 350 (2011) ("[T]here is another side to the value of the rule of law that is especially significant in the adversarial American system: law as a structured discourse in which individuals are entitled to articulate their grievances or face their accusers, to stake their claims, and to advance reasons in support of them.").

[195] Frederick Schauer, *Giving Reasons*, 47 STAN. L. REV. 633, 658 (1995) ("That giving reasons is a way of opening a conversation may in fact be an independent basis for a reason-giving requirement."); Ruger et al., *supra* note 192, at 1193 (noting that the Supreme Court's "role in American society is not merely to process important disputes expeditiously. Rather, the ways in which it addresses those disputes—not merely through outcomes, but through its rationales, its analytical framework, and its language—both gives voice to certain values and influences public understanding of these issues").

[196] Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED MAG. (June 23, 2008), https://www.wired.com/2008/06/pb-theory/ [https://perma.cc/5K49-B2CD]; Martin Hilbert, *Big Data for Development: From Information to Knowledge Societies* (SSRN Scholarly Paper No. 2205145, 2013), http://papers.ssrn.com/abstract=2205145 [https://perma.cc/ZX2H-284X].

[197] *See* Martin L. Weitzman, *Recombinant Growth*, 113 Q.J. ECON. 331, 331 (1998) ("Production of new ideas is made a function of newly reconfigured old ideas in the spirit of the way an agricultural research station develops improved plant varieties by cross-pollinating existing plant varieties.").

[198] Mike Orcutt, *Why IBM Just Bought Billions of Medical Images for Watson to Look at*, MIT TECH. REV. (Aug. 11, 2015), https://www.technologyreview.com/s/540141/why-ibm-just-bought-billions-of-medical-images-for-watson-to-look-at/ [https://perma.cc/A34D-8SZN].

Another set of problems created by the nature and process of automated prediction entails a lack of transparency. Like Big Data applications generally, most legal prediction programs give a user results without showing the precise combination of factors that produced those results.[199] Certainly, an application's programmers can view the code of the relevant inductive rule model, but the code is not always interpretable by the programmer, much less a lay person, and will frequently be proprietary, protected as a trade secret. Interpretability could be prioritized such that no outcome would be accepted—whether by a client, a lawyer, or a court—without a full explanation of inputs, but there is reason to doubt that this will happen. Requiring every outcome to be accompanied by a complete explanation of inputs (features that gave rise to the computer's model) would be exceedingly expensive and time consuming. Most users would not be willing to bear that expense. Moreover, interpretability might be a reasonable goal for applications that consider a modest amount of data, but as the universe of data expands to tens of thousands or millions of variables (words, linguistic features, data points), the goal of interpretability becomes more and more difficult, if not impossible.

This lack of transparency threatens a number of consequences over time. If clients increasingly rely on software predictions in determining a course of action—in deciding, for example, whether to file a complaint, to defend a case, or to pursue a particular corporate transaction—the software's predictions, by virtue of their influence over conduct, will influence the law in action. Without anyone realizing it, factors encoded into those predictions—including discriminatory or otherwise problematic factors—could then become encoded into broader swaths of law. For example, a computer might discover a weak correlation between a particular court's decisions and the gender, race, or ethnicity of the litigants. The estimated statistical model would then account for the correlation in predicting success or failure. Because the correlation is weak, the model's results might not immediately alert us to its influence in a way that would allow for accountability. Nevertheless, the discriminatory pattern would inform predictions of the court's decisions, and litigant behavior in the shadow of those decisions. There is also the possibility of the opposite—of technology being used to counter, rather than to entrench, human biases. One could imagine a sophisticated prediction model that produced race-neutral sentencing suggestions based only on the facts of the case. But any such use of prediction software would require coordinated attention and

[199] David Martens & Foster Provost, *Explaining Documents' Classification*, at 2 (N.Y.U. Stern Sch. of Bus., Working Paper No. CeDER-11-01, 2011), http://archive.nyu.edu/handle/2451/29918 [https://perma.cc/2YZJ-LNQF] ("Unfortunately, due to the high dimensionality, understanding the decisions made by the document classifiers is very difficult. Previous approaches to gain insight into black-box models do not deal well with high-dimensional data."); *see also* Tal Z. Zarsky, *Transparent Predictions*, 2013 U. ILL. L. REV. 1503, 1520 ("Yet interpretability has a flip side as well. Mandating interpretability might render the process less complex and therefore less accurate.").

action by a broad swath of implicated stakeholders, which would slow the current progress, pushed largely by one particular set of stakeholders—insurance companies and litigation financing firms, eager to gather better information about what cases to back and bring to trial.

3. ACCESS TO JUSTICE

Finally, amidst countless claims that technology alone can solve the access to justice gap,[200] we should remain cognizant that without regulation, the development and adoption of legal technologies will be driven by the market—a decidedly ineffective means of ensuring access.

Technology proponents contend that the emergence of services like LegalZoom demonstrates that the market is working better than the profession at providing legal services at the low end of the market. Those who cannot afford a lawyer, they contend, can now access computerized legal services for low or no cost, and surely some form of legal services is better than none.

This is undoubtedly true in some contexts, but it is not in others. For one thing, the computer may encounter an unanticipated contingency but fail to alert the user, creating an error with no notice. For another, the computer cannot exhibit creativity such that, at least for now, it cannot create novel legal arguments that may initiate change in the law. The result could be "a digital divide that institutionalizes a two-tiered system incapable of delivering appropriate justice to low-income persons."[201]

Technology designed for the top of the market can also pose access challenges. One can easily imagine a dispute or transaction in which one party has access to a particular legal technology while the other party does not. For example, the significant up-front costs of predictive coding, including the licensing fees for patented programs, may be prohibitive for one party but affordable for the other.[202] A resource imbalance between parties is nothing new, but the unequal access to technology may introduce new types of unfairness or even abuse. The party who cannot afford predictive coding will likely lack understanding of the technology and therefore be unable to challenge the proposed discovery approaches and predictive coding protocols of the opponent. Meanwhile, the party with predictive coding, aware that the other party lacks access and has limited resources to fund manual review, will have opportunities to hide relevant and damning documents amidst massive document productions.

This does not mean that technology should not or will not play an important role in addressing the access to justice gap but rather, it is to say that the

[200] *See supra* note 174.

[201] Cabral et al., *supra* note 11, at 257; *see* Julia R. Gordon, *Legal Services and the Digital Divide*, 12 ALB. L.J. SCI. & TECH. 809 (2002).

[202] *See* Remus, *Predictive Coding*, *supra* note 47.

profession has an important part to play in ensuring that legal technologies are made accessible and used in ways that contribute to, rather than undermine, universal access to the legal system. Segments of the profession are doing just this. For example, the California Administrative Office of the Courts commissioned a study of California legal services providers and self-help center staff to identify potential benefits and barriers that increased use of technology posed for low-income persons.[203] Among other things, the report recommended hybrid legal services systems, which integrate human and automated legal assistance.[204] A number of law schools across the country are offering courses in which students design web-based applications that make legal information accessible while explicitly informing the user that she is not receiving legal advice and should contact an attorney with questions (thus, taking the safe approach to unanticipated contingencies).[205] Northeastern law school has launched NULawLab, which involves students in a range of projects that use technology to make law more accessible to everyone.[206]

4. A THOUGHT EXPERIMENT

To further highlight why we believe that some form of professional oversight and regulation of new legal technologies is essential, we offer a simple thought experiment. Suppose that new software can accurately predict the likelihood that an individual will be audited by the Internal Revenue Service (IRS) and, if audited, that the proposed tax treatment of an asset-sheltering trust will be upheld. Suppose further that the software offers each prediction as a numerical probability, and there are no error costs. It is marketed to, and widely adopted by, financial planners who serve wealthy clients interested in minimizing gift and estate taxes.

What will be lost if this software eclipses the advice of tax and estate planning lawyers, such that the values, norms, and structures of the legal profession are cut out of the equation? Answering this question highlights value that lawyers provide and that, at least for the time being, computers cannot:

[203] JUD. COUNCIL OF CAL. CT. TECH. ADVISORY COMM., ADVANCING ACCESS TO JUSTICE THROUGH TECHNOLOGY: GUIDING PRINCIPLES FOR CALIFORNIA JUDICIAL BRANCH INITIATIVES (2012). The report recognized that "[b]ecause so many cases now involve self-represented parties, technology must be implemented in ways that benefit those with or without legal representation so that all parties have equal access to the courts." *Id.* at 5.

[204] *Id.* at 7–8.

[205] Rostain et al., *supra* note 174, at 744.

[206] For example, an online game prepares individuals to represent themselves in court, *see, e.g.*, *RePresent: Online Game for Self-Represented Litigants*, NULAWLAB, http://www.nulawlab.org/view/online-simulation-for-self-represented-parties [https://perma.cc/872G-A26D] (last visited Mar. 10, 2017); a mobile phone app provides underserved women veterans with information about their legal rights and available benefits, *see, e.g.*, *Women Veterans Outreach Tool*, NULAWLAB, http://www.nulawlab.org/view/women-veterans-outreach-tool [https://perma.cc/7DCR-9P6T] (last visited Mar. 10, 2017); and an automated hotline informs domestic workers in the Boston area of their legal rights, *see, e.g.*, *The Worker App*, NULAWLAB, http://nulawlab.org/view/the-domestic-worker-app [https://perma.cc/U22A-AJBV] (last visited Mar. 10, 2010).

- Counseling. The tax software can predict how the IRS will act, but it cannot and will not counsel the taxpayer on how to proceed, including on the value of compliance and the possibility of an alternative course of action.[207] Nor can it push back against a taxpayer who insists on proceeding with an illegal scheme, notwithstanding the fact that, as Elihu Root famously asserted, sometimes the proper role of the lawyer is to tell clients "that they are damned fools and should stop."[208]
- A robust understanding of law. Individuals planning their affairs pursuant to the software's prediction will come to experience the law purely in terms of what conduct will and will not be sanctioned—"what the courts will do in fact, and nothing more."[209] This impoverished view of the law will have detrimental consequences not only for compliance,[210] but also for perceptions of the legal system's legitimacy and democratic participation in lawmaking.[211]
- Respect for clients' interests. The software objectifies a user[212] by assuming that the objective of all users is to use any asset-sheltering trust arrangement for which the projected savings outweigh the risk of detection. Some individuals engaged in estate planning seek excessively aggressive strategies, but others simply want to ensure that they are not needlessly sacrificing assets that could be shielded under well-settled law. The software simply ignores this, projecting one set of interests onto all clients.[213]

[207] Deborah L. Rhode, *The Profession and the Public Interest*, 54 STAN. L. REV. 1501 (2002) ("One of the most crucial functions of legal counsel is to help individuals evaluate short-term economic objectives in light of long-term reputational concerns and to live up to their best, not worst instincts."); Harold Williams, *Professionalism and the Corporate Bar*, 36 BUS. LAW. 165–66 (1980).

[208] Deborah L. Rhode, *Moral Counseling*, 75 FORDHAM L. REV. 1317, 1321 (2006) (quoting PHILIP C. JESSUP, 1 ELIHU ROOT 133 (1938)); *see also* RHODE, INTERESTS OF JUSTICE, *supra* note 100; Wendel, *Professionalism as Interpretation*, *supra* note 100; Gordon, *New Role for Lawyers?*, *supra* note 100; Rostain, *Ethics Lost*, *supra* note 100, at 1274–75.

[209] Holmes, *supra* note 193, at 460–61.

[210] Robert W. Gordon, *A Collective Failure of Nerve: The Bar's Response to Kaye Scholer*, 23 LAW & SOC. INQUIRY 315 (1998) ("[T]he order of rules and norms, policies and procedures, and institutional actors and roles that make up the legal system . . . is only as effective as voluntary compliance can make it; for if people routinely start running red lights when they think no cop is watching . . . the regime will collapse."); Stephen Pepper, *Counseling at the Limits of the Law: An Exercise in the Jurisprudence and Ethics of Lawyering*, 104 YALE L.J. 1545, 1547–48 (1995) ("In a complex legal environment much law cannot be known and acted upon, cannot function as law, without lawyers to make it accessible to those for whom it is relevant."); W. Bradley Wendel, *Legal Ethics As "Political Moralism" or the Morality of Politics*, 93 CORNELL L. REV. 1413, 1417–18 (2008).

[211] Wendel, *Professionalism as Interpretation*, *supra* note 100, at 1173 ("[T]he law cannot operate as a device to settle normative conflict and coordinate activity without a commitment on the part of law-interpreters to respect the substantive meaning standing behind the formal expression of legal norms.").

[212] Simon, *supra* note 99, at 53–54 (warning that lawyers who adhere to the dominant ideology of professionalism "impute certain basic aims to the client," which tend to be legalistic and to "emphasize extreme selfishness"); Kruse, *Client-Centered Norms*, *supra* note 99, at 346.

[213] And yet, as Kate Kruse and others have persuasively argued, lawyers can and should work to advance and represent their clients' interests, understood holistically; not the interests that they or the legal system

- Access to reasons. The tax software, like most Big Data applications, offers no reasons for its predictions. And yet, reasons, from lawyers as much as from judges,[214] are a critical source of both stability and change in the law[215] and a critical expression of respect for participants in the legal system.[216] Without reasons, neither the taxpayer nor the financial planner could understand the law so as to follow it or extrapolate the result to similar cases.[217] Nor could they critique the result, or argue for change.[218]
- Interaction with the legal system. Finally, widespread displacement of estate and tax lawyers by prediction software would eliminate a critical mechanism through which the state and society interact.[219] Lawyers translate their clients' interests into terms the legal system can understand and act upon, and the law into terms that their clients can understand and act upon.[220] Here, a lawyer could educate a taxpayer regarding the IRS's regulatory goals, and suggest an arrangement that would still minimize taxes without thwarting those goals. Or the lawyer could represent the taxpayer's interests in challenging the IRS's treatment of a particular arrangement or interpretation of a particular Code provision.

In some contexts, and with regards to some technologies, the benefits of decreased expense and increased certainty and determinacy in the law may outweigh, or may be achievable without, the costs. Moreover, the costs are those of eliminating lawyers entirely, and not a necessary consequence of the technologies themselves. The import of our thought experiment is not, therefore, to condemn legal technologies. Rather, it is to show the importance of ensuring that their development, adoption, and use are governed by norms and regulations that align with the underlying values of our legal system.

project onto clients. Kruse, *Beyond Cardboard Clients*, *supra* note 99, at 127–28 (describing client-centered lawyering, which entails "hearing clients' stories and understanding their values, cares, and commitments," as an answer to the problem of legal objectification); DAVID A. BINDER ET AL., LAWYERS AS COUNSELORS: A CLIENT-CENTERED APPROACH 2–15 (1991).

[214] Wendel, *Professionalism as Interpretation*, *supra* note 100, at 1169–70 (discussing professionalism as "demand[ing] that lawyers provide a public, reasoned justification for an interpretation of legal texts—one which is plausible in light of the interpretive understandings of a professional community.").

[215] David Luban, *Natural Law as Professional Ethics: A Reading of Fuller*, *in* NATURAL LAW AND MODERN MORAL PHILOSOPHY 176, 204 (Ellen Frankel Paul et al. eds., 2001).

[216] *See* Schauer, *supra* note 195, at 656; Luban, *supra* note 215, at 110–11 (discussing Fuller's distinction between law and managerial direction, and view that the former implies "a certain built-in respect for [the] human dignity" of those subject to the law).

[217] Schauer, *supra* note 195, at 641 ("When we provide a reason for a particular decision, we typically provide a rule, principle, standard, norm, or maxim broader than the decision itself, and this is so even if the form of articulation is not exactly what we normally think of as a principle.").

[218] *Id.* at 658.

[219] *See* DANIEL MARKOVITS, A MODERN LEGAL ETHICS: ADVERSARY ADVOCACY IN A DEMOCRATIC AGE 171–200 (2008).

[220] Remus, *Reconstructing Professionalism*, *supra* note 10, at 37.

5. A MORE MEANINGFUL APPROACH TO REGULATION

A roadmap for regulatory reform is beyond the scope of this Article and is a task for future work. For now, we propose proportionality as the guiding principle. Not all existing and emerging software will perform a task as well as—much less better than—a human lawyer. That is not a necessity for adoption, however, given that most software is likely to perform tasks more cheaply than a human lawyer. The issue is one of proportionality: is the less-than-human performance adequate for the task at hand, particularly given the lower cost?

The principle of proportionality recognizes that in certain contexts, lowered quality may be an acceptable and desirable tradeoff in service of increased access; in other contexts, it will not be. Many potential clients may feel that an expert system to address routine compliance or an online service provider to draft a basic will provide the level of service they want and need even if the system is not able to analyze problems as completely as a skilled human lawyer. These clients may feel that the more detailed analysis by a human lawyer does not justify its cost. Many potential clients may receive services through an expert system, such as the DoNotPay program that contests parking tickets for free, that they never could or would have received from a lawyer with little or no offsetting risk.[221] But clients may feel differently in other contexts, such as in the courtroom or in a child custody battle. More generally, task automation may impose a degree of standardization that loses a degree of human nuance, but the nuance may not be important for many potential users.

This, in turn, raises the key questions of client identity and autonomy. Who should make the decision of where and when these tradeoffs are acceptable? As a predictive matter, the bar has been much more willing to acquiesce to acceptance of risk by sophisticated and corporate users of legal services than by first-time individuals, but it is generally the latter who need more affordable legal services and may be the most eager for the tradeoff of proportionality. It is also the latter who are the targeted clients of new technologies that are offered without lawyer supervision, such as LegalZoom, and for whom the consumer protection rationale of regulation may be essential. Accordingly, we think these decisions cannot be entirely left to clients. We think there must be a role for regulatory bodies, populated largely though not exclusively by lawyers.

To make informed regulatory decisions, lawyers generally and bar committees in particular will have to become more informed and more skilled with new legal technologies. Both groups will also need to struggle with the bounds of the "practice of law" and with the increasingly mixed nature of legal expertise and

[221] "In the 21 months since the free service was launched . . . DoNotPay has taken on 250,000 cases and won 160,000, giving it a success rate of 64% appealing over $4m of parking tickets." Gibbs, *supra* note 95. The creator plans to expand to address flight delay compensation, rights of HIV positive individuals, and refugees navigating foreign legal systems.

other forms of expertise. Only by doing so will the bar be able to adjust to current realities and fulfill its obligation to society.

CONCLUSION

At the risk of oversimplifying, we think it is fair to characterize much of the current debate regarding legal technologies as existing at the extremes. With respect to employment effects, headlines proclaim the end of the legal profession. Traditionalists respond with unauthorized practice of law rules, arguing that new technologies threaten client interests and undermine the core values of the profession. Many scholars and commentators push back, arguing that we should automate as many legal services as possible in an attempt to reduce prices and increase access.

This Article has sought to add detail and nuance to the discussion. First, we showed that while technology is undoubtedly advancing and changing the nature of legal practice, it is displacing lawyers at a modest pace. Second, we argued that while current approaches to the professional regulation of legal technologies are ineffective and undesirable, the answer cannot be to abandon professional regulation. Instead, we must begin the difficult but important task of designing more effective regulatory structures that draw upon both legal and technical expertise, while protecting both clients and the values of our legal system.

APPENDIX

APPROXIMATE ESTIMATES OF MODERATE AND LIGHT EMPLOYMENT EFFECTS

Moderate Employment Effects: As noted above, moderate employment effects arise when a largely unstructured legal task has a significant structured component that can be computerized. To calibrate the employment impact of this level of innovation, we refer to a case study of search-related innovation in exceptions processing at a large bank.[222] Exceptions processing requires determining the proper disposition of

> checks written on accounts that have been closed, checks written for amounts greater than the balances in the accounts on which they are drawn, checks that customers request stop payments on, checks written for large amounts that require signature verification, and fraudulent checks.[223]

Each department employee reconciled a single type of exception. The work was made more complex because a single check could involve multiple exceptions. For example, individuals short of cash might buy time by writing multiple checks to creditors and by then submitting multiple stop-check orders. The result was substantial time spent both searching boxes of checks for particular items and coordinating work among employees addressing different exceptions for the same account.

When digital check images were substituted for paper checks in the workflow, employees who handled exceptions gained rapid access to a particular check, resulting in reduced search time and, therefore, increased productivity. Simultaneously, the exceptions departments reorganized their workflow such that employees no longer focused on a particular type of exception but instead handled all exceptions for a particular set of accounts.

This new technology and reorganization, which could have taken place with paper checks (though it did not), increased productivity. The combined effect was to reduce the number of employees required to handle a constant volume of exceptions from 650 to 470—a reduction of twenty-eight percent. A computer-friendly estimate attributes two-thirds of this reduction to the digitized images and one-third to the reorganization. Correspondingly, we assume that lawyering tasks in which computers have a Moderate Employment Effect reduce lawyer time devoted to those tasks by nineteen percent.

Light Employment Effects: This category includes tasks that entail largely unstructured work with limited room for automation—e.g., Fact Investigation or

[222] *See* Autor et al., *supra* note 22, at 437.
[223] *Id.*

Advising Clients.[224]

To calibrate Light Employment Effects, we use a case study of a limited computer innovation in healthcare: Adler-Milstein and Huckman's study of the impact of electronic medical record (EMR) use on clinician productivity.[225] Productivity in the study is measured by "Relative Value Units" billed per clinician workday, which is the standard medical accounting measure of the volume and intensity of services provided. The study's sample consists of forty-two medical practices, which were observed over three years during which they implemented EMRs at various rates. Findings indicate that one standard deviation in the use of an EMR increases clinician productivity by five percent. Services per patient visit did not increase, but physicians could see more patients per workday by using the EMR to delegate some services to physicians' assistants. Relying on this example, we posit that adopting a computer innovation with Light Employment Effects would decrease required lawyer employment for a given task by five percent.

[224] Light employment effects also arise in tasks relating to document management. Because these tasks are usually performed by clerical staff, automation does not affect lawyer employment per se.

[225] Adler-Milstein & Huckman, *supra* note 125.

Topic V

Technology Assisted Review for eDiscovery

CHAPTER 3

A Tour of Technology-Assisted Review

Maura R. Grossman and Gordon V. Cormack

Introduction

Since the publication of our 2011 article, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review*, in the Richmond Journal of Law and Technology (JOLT article),[1] the term "technology-assisted review" (TAR)—along with related terms such as "computer-assisted review" (CAR) and "predictive coding" (PC)—has been used extensively in writings, presentations, and legal documents to advance or assail a plethora of tools and methods aimed at decreasing the cost and burden associated with document review in electronic discovery (e-discovery). The conflation of diverse tools and methods under a single label has resulted in confusion in the marketplace, and inapt generalizations regarding the effectiveness (or ineffectiveness) and proper use of such tools and methods. In this chapter, we outline and illustrate—using a running example—the principal distinctions among the various tools and methods that we consider to be variants of TAR, and differentiate them from other tools and methods, such as concept search, clustering, visualization, and social network analysis, which we do not consider to be TAR. While e-discovery tools fall on a continuum in terms of their utility for search, analysis, and review, we describe certain components that, in our opinion, are essential for a tool to be considered "technology-assisted review."

Distinguishing Among Search, Analysis, and Review

Search, analysis, and review are different tasks with different objectives. The objective of search is to find enough documents to satisfy an information need, such as the answer to a question or support for a proposition. The objective of analysis is to gain understanding from available data, so as to support decision-making. The objective of review is to classify all documents in a collection as meeting—or not meeting—certain criteria, such as responsive to a request for production, subject to attorney–client privilege or work–product protection, or available for disposal. Following information retrieval practice, in this chapter, we refer to documents meeting the review criteria as "relevant," and those not meeting the criteria as "nonrelevant," although in the legal domain, this distinction is sometimes referred to as "responsive" and "nonresponsive."

While there is some overlap between the tools and methods used for search and analysis, and those used for review, we apply the term "technology-assisted review" or "TAR" only to tools and methods used specifically for review.

Almost everyone is familiar with Web search engines like Google, Bing, and Yahoo!, and the ease with which they may be used to find a few relevant documents in response to an information need. Search engines, however, are much less amenable to the task of finding all, or nearly all, relevant documents, as required for review.

Analytic tools such as clustering, visualization, and social network analysis may yield insights leading to the discovery of relevant documents, but, like search engines, they are not in and of themselves well-suited to review.

Search, analytic, and review tools are often combined in commercial document review platforms to provide a suite of options to deal with the large collections of data that are commonly encountered in e-discovery in legal and regulatory investigations or proceedings. The components of these offerings are not always susceptible to easy labels because, in reality, tools used for search, analysis, and review can fall on a continuum, and many e-discovery approaches rely on ad-hoc, hybrid methods that move in iterative cycles among search, analysis, and review.

Defining Technology-Assisted Review and Distinguishing Rule-Based from Supervised Machine-Learning Approaches to TAR

Methods used for technology-assisted review may be broadly classified into those employing rule bases and those employing supervised machine learning. A rule base consists of a large set of rules, composed by one or more subject-matter and rules-construction experts, to separate documents meeting the criteria for relevance, from those that do not. These rules may take the form of complex Boolean queries—specifying combinations of words and their order or proximity—that indicate relevance or nonrelevance, exceptions to those rules, exceptions to the exceptions, and so on, until nearly all documents in the collection are correctly classified. Supervised machine learning, on the other hand, infers, from exemplar documents, characteristics that indicate relevance or nonrelevance, and uses the presence or absence of those features to predict the relevance or nonrelevance of other documents.

Our 2011 JOLT article compared the effectiveness of a rule-based TAR method (H5) and a supervised machine-learning TAR method (Waterloo) to that of human review, concluding that both of these TAR methods were able to equal or exceed the effectiveness of human review—as measured by recall, precision, and F^1—with a small fraction of the human review effort. Since its publication, a number of service providers have cited the JOLT article as support for the efficacy of their own tools or methods, under names such as "technology-assisted review," "computer-assisted review," "assisted review," "language-based analytics," and "predictive coding," among others. Many of these approaches, however, bear little resemblance to the two methods studied in our JOLT article.

It is important to note that there is no standards-setting or regulatory body controlling the application of these terms to various tools and methods, and therefore, there is no guarantee that a tool labeled "TAR," or "predictive coding," or "language-based analytics" employs any particular method, or that the method it does employ—whether aptly named or not—is effective for review. Nevertheless, because a common vocabulary is essential to rational discourse, to this end, in 2013, we published a glossary of terms in Federal Courts Law Review (the Glossary),[2] which we will augment in this chapter, to taxonify current methods used for technology-assisted review. (This glossary also appears as the appendix of this book.) The Glossary defines technology-assisted review (TAR) as:

> A process for Prioritizing or Coding a Collection of Documents using a computerized system that harnesses human judgments of one or more Subject Matter Expert(s) on a smaller set of Documents and then extrapolates those judgments to the remaining Document Collection. Some TAR methods use Machine Learning Algorithms to distinguish Relevant from Non-Relevant Documents, based on Training Examples Coded as Relevant or Non-Relevant by the Subject Matter Experts(s), while other TAR methods derive systematic Rules that emulate the expert(s)' decision-making process. TAR processes generally incorporate Statistical Models and/or Sampling techniques to guide the process and to measure overall system effectiveness.

We intended this definition to exclude search and analytic tools per se because they do not extrapolate relevance judgments to the collection. Certainly, one could use a search tool for review, by deeming all nonretrieved documents to be nonrelevant. Similarly, one could use a clustering tool for review by deeming all members of each cluster, as a group, to be either relevant or nonrelevant. However, neither approach has been shown to be effective for review; thus, to label an underlying search engine or clustering method as a "TAR" tool would, in our view, weaken the definition of TAR so as to render it meaningless. We suggest that it would be more fruitful to label methods as "TAR" only if they rank or make affirmative predictions about the relevance or nonrelevance of documents in the collection based on human judgments that are applied to a subset of the collection. Rule-based and supervised machine-learning methods meet this definition because they generate rules or mathematical models that discriminate between relevant and nonrelevant documents.

The Path from Keyword Search to TAR

When one tries to delineate the precise boundary between what is and is not TAR, it becomes apparent that this distinction is not entirely clearcut; rather, methods fall on a continuum from those geared more toward search and analysis, to those geared more toward review. Accordingly, it seemed to us that the best way to explain TAR would be to begin with keyword search and to walk through the process of adding additional technological components that start to convert a search method into technology-assisted review. We thought it might also be useful to demonstrate these different components using a common example to illustrate their relative effectiveness, or ineffectiveness, for review.

A Running Example: Fantasy Football

To illustrate the evolution of methods from simple keyword search to TAR, we use as a running example Topic 207 from the TREC 2009 Legal Track, which was reprised in the TREC 2010 Legal Track, and used again, as a practice example, in the TREC 2015 Total Recall Track.[3] Topic 207 requires the identification of,

> [a]ll documents or communications that describe, discuss, refer to, report on, or relate to fantasy football, gambling on football, and related activities, including but not limited to, football teams, football players, football games, football statistics, and football performance[,]

from a set of documents collected from Enron Corporation by the Federal Energy Regulatory Commission. The particular collections used for TREC 2009 and TREC 2010 are no longer publicly available; for this example, we used the collection supplied to participants with the baseline model implementation (BMI) for the TREC 2015 Total Recall Track.[4] This collection contains 723,386 documents, of which (unbe-knownst to our hypothetical searcher) 7,798, or about 1.1 percent, are relevant to Topic 207.

Basic Keywords or Search Terms

To identify documents concerning fantasy football, our hypothetical searcher might simply begin by selecting all documents containing the word "football"—a task that is readily accomplished using the search feature in most document review platforms. Most likely this search would yield a substantial number of documents concerning actual football teams, players, games, and statistics, but it would also be likely to identify documents with metaphorical, humorous, and other uses beyond those specified by Topic 207. In our example, again unbe-knownst to our searcher, the term "football" selects 4,319 documents from the corpus, of which 3,480 are relevant, and 839 are not. In other words, a search for "football" has 44.6 percent recall (where "recall" is defined as the fraction of all relevant documents in the collection identified by the search; in this case 3,480/7,798 = 44.6 percent), and 80.6 percent precision (where "precision" is defined as the fraction of the documents identified by the search that are relevant; in this case 3,480/4,319 = 80.6 percent).

Without additional testing or inquiry, our searcher would have no way of knowing what level of recall and precision her search had achieved, and therefore no tool other than her intuition to assess the adequacy of her search.[5] Human intuition concerning the adequacy of keyword search, however, has been shown to be woefully inadequate. In a seminal 1985 study,[6] Blair and Maron asked skilled paralegals, supervised by lawyers, to use search terms to find documents responsive to each of 51 requests. Although the lawyers and paralegals believed they had achieved an adequate result—which they defined to mean having achieved recall of at least 75 percent—they had, in fact, achieved recall of only 20 percent, on average. No more recent study that we are aware of has shown human intuition about search terms to have improved since then.

Control Sets

The first step in the transition from search terms to TAR would involve the addition of a principled mechanism to ensure that a substantial majority of the relevant documents were identified by the process. To this end, many processes rely on statistical sampling to estimate how many relevant documents there are to be found in the collection, how many relevant documents have been identified by a particular search or review strategy, and thus, the recall and precision of that strategy. A common (but not universal) approach is to use a random sample taken at the outset of the process, known as a "control set," to estimate these quantities, and thereafter to guide the process, or to validate its effectiveness.

Each document in the control set is reviewed and coded as relevant or not by a subject-matter expert (SME). The fraction of relevant documents in the control set provides an estimate of the fraction of relevant documents in the collection, with some margin of error. This proportion is referred to as "prevalence."[7] Provided that the control set is independent of the search effort—that is, no information about the search is used in choosing and coding the control set, and no information about the content or coding of the control set is used in devising the search strategy—the control set may be used to yield valid estimates of the recall and precision of the search or review process.[8]

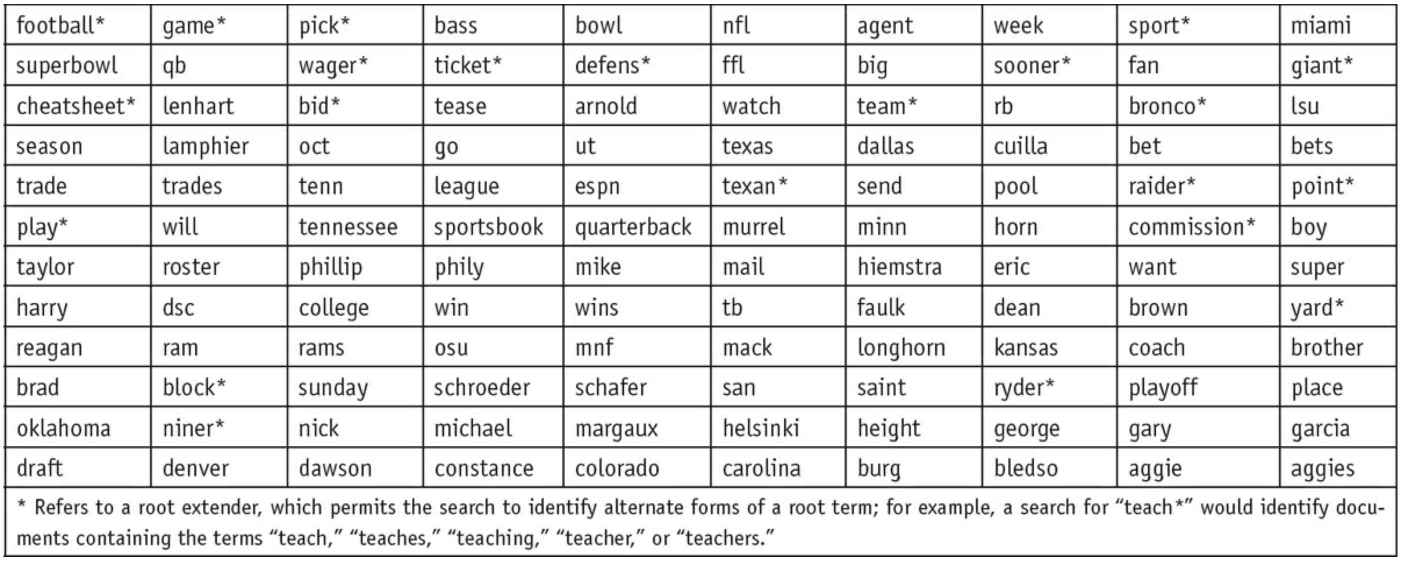
For our running example, we chose a control set consisting of 3,000 random documents. We found that 31 of the 3,000 documents (1.03 percent) were relevant to Topic 207, and therefore assume that approximately 1.03 percent of the collection (7,473 documents) is likely to be relevant. This estimate is reasonably close to the true value of 1.08 percent (7,798 documents). Furthermore, 17 of the 20 "hits" for the term "football" in the control set are relevant, yielding a precision estimate of 85.0 percent, and a recall estimate of 64.5 percent. While the recall estimate is considerably higher than the true value of 44.6 percent, it is still within the margin of error one might expect for a sample of this size.

Combining Search Terms

A single search term is rarely sufficient to capture substantially all relevant documents in a collection. For Topic 207, the term "football" identified 44.6 percent of the responsive documents; the problem remains of how to identify the remaining 55.4 percent. Assuming that it is determined—either by intuition, statistics, or otherwise—that it is necessary to find more relevant documents, an obvious choice would be to add additional search terms; a less obvious choice is *which* search terms to use. Table 3.1 contains 120 possible search terms our searcher might incorporate into her keyword search. Which would you pick?

If we knew, for example, that the term "NFL" selected 1,666 documents, of which 1,542 were relevant, we might be inclined to include this term. But 1,261 of these documents were already selected by the term "football," so the net effect is that "NFL" identifies only 281 new responsive documents, at the expense of 106 new nonresponsive ones. Knowing this, should our searcher still include the term "NFL"?

TABLE 3.1 120 Candidate Search Terms Related to TREC Topic 207 (Fantasy Football)



football*	game*	pick*	bass	bowl	nfl	agent	week	sport*	miami
superbowl	qb	wager*	ticket*	defens*	ffl	big	sooner*	fan	giant*
cheatsheet*	lenhart	bid*	tease	arnold	watch	team*	rb	bronco*	lsu
season	lamphier	oct	go	ut	texas	dallas	cuilla	bet	bets
trade	trades	tenn	league	espn	texan*	send	pool	raider*	point*
play*	will	tennessee	sportsbook	quarterback	murrel	minn	horn	commission*	boy
taylor	roster	phillip	phily	mike	mail	hiemstra	eric	want	super
harry	dsc	college	win	wins	tb	faulk	dean	brown	yard*
reagan	ram	rams	osu	mnf	mack	longhorn	kansas	coach	brother
brad	block*	sunday	schroeder	schafer	san	saint	ryder*	playoff	place
oklahoma	niner*	nick	michael	margaux	helsinki	height	george	gary	garcia
draft	denver	dawson	constance	colorado	carolina	burg	bledso	aggie	aggies

* Refers to a root extender, which permits the search to identify alternate forms of a root term; for example, a search for "teach*" would identify documents containing the terms "teach," "teaches," "teaching," "teacher," or "teachers."

As more search terms are used, it becomes increasingly difficult to choose additional terms that select many new, relevant documents, and few nonrelevant ones. There are approximately 10^{40} (i.e., 1 followed by 40 zeros) possible combinations of the terms in Table 3.1. The chance of finding the best combination of them, through intuition alone, is remote.

We could use our control set for this purpose, but once we use the control set to aid our search strategy, it is no longer independent, and therefore ceases to be a valid statistical sample for estimating recall and precision for validation purposes. When the selection of search terms is done with the benefit of feedback derived from the control set, terms may be selected that correctly identify the relevant documents in the control set, but not necessarily in the rest of the collection. This phenomenon is known as overfitting.[9]

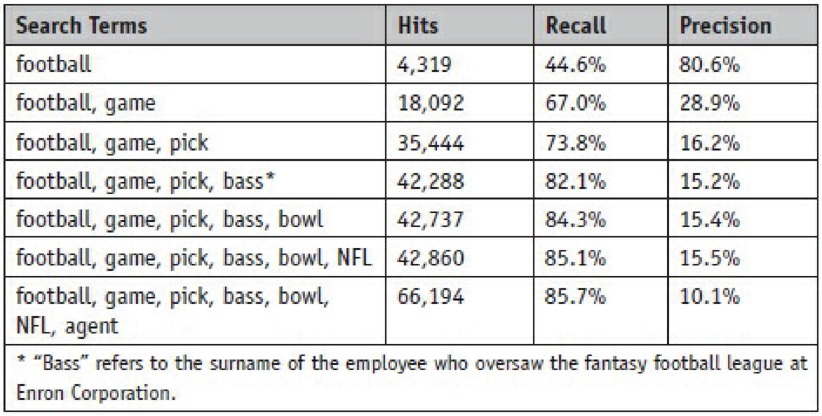
When a set of documents is coded and used to guide the selection of keywords—or any other aspect of the search or review process— such a set is more properly referred to as a "training set." The systematic use of a training set is a key factor that distinguishes TAR from search.

For the purpose of illustrating a carefully crafted set of keywords, we selected the terms in Table 3.1, and ordered them by their estimated effectiveness (from left to right, by row), using an algorithm and a training set.[10] While we have no empirical evidence to support our claim, we posit that a human reviewer relying solely on her intuition would be hard-pressed to come up with a better list; we therefore use this list to model the best possible result that could be achieved with reasonable effort. But, even given this list of terms, the question still remains: How many of the "best possible" terms should be used for the search?

As we have seen, the term "football," alone, yields 44.6 percent recall and 80.6 percent precision. The terms "football" and "game," together, yield 67.0 percent recall and 28.9 percent precision. In other words, it is necessary to review 18,092 documents—13,773 more than the 4,319 selected by "football" alone—to raise recall from 44.6 percent to 67.0 percent. In the extreme, the 120 search terms combined select 570,466 documents, or about 80 percent of the collection, achieving 99.7 percent recall, but only 1.4 percent precision.

Table 3.2 illustrates the recall-precision trade-off that ensues from using various combinations of search terms. The first column (Search Terms) shows increasingly large sets of the "best possible" search terms selected from Table 3.1. The second column (Hits) shows the number of documents selected by the set of search terms, representing the amount of effort that would be required to review all documents selected by the search terms. The third and fourth columns (Recall and Precision, respectively) show the recall and precision of the search.

TABLE 3.2 Hit Counts, Recall, and Precision for Various Combinations of High-Quality Search Terms



Search Terms	Hits	Recall	Precision
football	4,319	44.6%	80.6%
football, game	18,092	67.0%	28.9%
football, game, pick	35,444	73.8%	16.2%
football, game, pick, bass*	42,288	82.1%	15.2%
football, game, pick, bass, bowl	42,737	84.3%	15.4%
football, game, pick, bass, bowl, NFL	42,860	85.1%	15.5%
football, game, pick, bass, bowl, NFL, agent	66,194	85.7%	10.1%

* "Bass" refers to the surname of the employee who oversaw the fantasy football league at Enron Corporation.

It is easy to see that using more search terms increases recall at the expense of increased effort (and, correspondingly, decreased precision). No matter how carefully search terms are selected, high recall can be achieved only at the expense of low precision, which translates to greater review effort.[11] It is therefore unlikely that a human, selecting search terms using her intuition alone, could guess a set of search terms that would yield higher recall and higher precision than any of the searches proposed in Table 3.2.

Boolean and Proximity Operators

The search tools incorporated in most document review platforms allow a searcher to combine search terms using Boolean operators, such as "AND," "OR," and "BUT NOT," as well as proximity operators, such as "FBY [followed by] *n*" or "WITHIN *n*." In this chapter, we refer to a combination of one or more search terms using Boolean operators as a "Boolean expression," and a combination of one or more search terms using Boolean and proximity operators as an "extended Boolean expression."

The simplest Boolean expression is a single search term that selects all documents containing it, but Boolean expressions can consist of more than one search term. Two Boolean expressions, E_1 and E_2, may be combined as follows:

- "E_1 OR E_2" selects all documents that contain *either* "E_1" *or* "E_2";
- "E_1 AND E_2" selects all documents that contain *both* "E_1" *and* "E_2";
- "E_1 BUT NOT E_2" selects all documents that contain "E_1," *but only if they do not contain* "E_2."

Boolean expressions may be extended by including pairs of search terms, T_1 and T_2, combined as follows:

- "T_1 FBY *n* T_2" selects all documents containing the term "T_1" followed by the term "T_2," separated by no more than *n* words;
- "T_1 WITHIN *n* T_2" selects all documents containing both terms "T_1" and "T_2," in either order, separated by no more than *n* words.

In the following discussion, we refer to Boolean and extended Boolean expressions collectively as "Boolean expressions," or, when used for searching, as "Boolean queries." The use of Boolean queries to select documents is referred to as "Boolean search."

Boolean queries allow searchers to particularize the documents selected by search terms. For example, if the term "game" selects a large number of documents about video games, as opposed to football, our searcher might use the Boolean query "game BUT NOT video." Constructing a Boolean query to achieve high recall and high precision is a formidable task that requires testing and iteration. A set of Boolean queries that is systematically constructed with the objective of selecting all and only the relevant documents is a form of rule base, discussed later in this chapter.

Relevance Ranking

As defined in our Glossary, relevance ranking is "[a] search method in which the results are ranked from the most likely to the least likely to be Relevant to an Information Need. . . ."[12] A familiar example of relevance ranking is Web search: A user types a few keywords into a search engine such as Google, Bing, or Yahoo! and receives, as a result, the top-ranked documents from millions of possible hits. These top-ranked documents are those that the search engine's relevance-ranking algorithm determines are most likely to contain the information that the user is seeking. Some (but not all) commercial document review platforms include relevance ranking, but, for reasons that are not entirely clear to us, relevance ranking is seldom used in e-discovery.

Using relevance ranking with a broad set of search terms (such as those in Table 3.1) is an effective alternative to the use of a narrow, carefully selected set of keywords alone (such as those in Table 3.2). To show this, we fed the 120 search terms listed in Table 3.1 to a well-known relevance-ranking algorithm (i.e., BM25, as implemented by the Wumpus Search software[13]) and achieved results—shown in Table 3.3—which are nearly as good as those achieved by our carefully crafted search terms using an automated method.[14] Table 3.3 shows the recall and precision that would be achieved if various numbers of the top-ranked documents were selected from the collection. The first column (# Top-Ranked Documents) reflects review effort, and is directly comparable to the second column (Hits) of Table 3.2. We can see, in our relevance-ranking example, that selecting the top-ranked 18,092 documents achieves 65.3 percent recall and 28.2 percent precision, whereas, in our keyword-search example, selecting 18,092 documents using the search terms "football" and "game" achieves 67.0 percent recall and 28.9 percent precision.

When using relevance ranking, the key decision that needs to be made—beyond identifying a broad set of search terms—is how many of the top-ranked documents should be selected so as to achieve the desired trade-off between recall and precision (i.e., completeness versus review effort). Although the precise recall and precision measures shown in Table 3.3 can be known only with clairvoyance, they could be estimated using a control set.

TABLE 3.3 Relevance Ranking for 120 Search Terms: Recall and Precision at Various Cut-Off Points

# Top-Ranked Documents	Recall	Precision
4,319	41.4%	74.8%
18,092	65.3%	28.2%
35,444	75.1%	16.5%
42,860	77.7%	14.2%
66,194	83.7%	9.9%

Relevance ranking is a fully automated technique that performs about as well as the best combination of keywords that we were able to construct using a combination of technology, knowledge of the collection, and hindsight, and almost certainly better than any combination of keywords whose selection was based solely on human intuition. Nonetheless, the use of relevance ranking remains relatively uncommon in the e-discovery community. Some of the resistance to its use may be due to the fact that the mechanism behind relevance ranking is not as easily understood as the mechanism behind keyword search, a property sometimes referred to as "transparency." It is important to note, however, that familiarity with the nuts and bolts of a method does not confer any information about the *effectiveness* of that method for its intended purpose. The same sense of familiarity may have led the lawyers and paralegals who participated in the Blair and Maron study to believe they had achieved 75 percent recall when they had achieved only 20 percent.

Similarity Search

Moving further down the path from search tools to TAR, there are a number of methods that seek to identify documents that are similar to a given document, or to one of a given set of documents, for some definition of "similar." These tools are often informally referred to as "find [me] more like this." In essence, the document or documents of interest assume the same role as search terms in a keyword search, and the challenge of choosing a good set of documents—often referred to within the context of similarity search as a "seed set"—parallels the challenge of finding a good set of search terms. There is a common misconception that knowledge of the seed set confers information about the effectiveness of the similarity search, much as there is an unfounded belief that knowledge of the search terms conveys information about the effectiveness of the keyword search. In both cases, the searcher does not know what she does not know, and transparency regarding the search mechanism does not change that. Replacing the unprincipled choice of search terms with the unprincipled choice of seed documents is no less a game of Go Fish.[15]

Many notions of "similar" are employed in similarity search tools. Similarity may be expressed in terms of a similarity measure (e.g., X percent) that indicates the degree of similarity between two documents. Alternatively, similarity may be expressed as the "distance" between two documents, where a larger distance means less similarity. Similarity search identifies any document that is more similar (or nearer) to a given document than some threshold value. Most similarity search tools allow this threshold to be adjusted, in much the same way that the cut-off for relevance ranking can be adjusted to vary the trade-off between recall and precision.

The most widely used similarity measures include cosine similarity and, more generally, the vector-space model (VSM), which are based on the words that appear in the documents (typically after stemming, stop-word elimination, and tf-idf (term frequency-inverse document frequency) weighting[16]).

Table 3.4 shows the results of a "find similar" search using cosine similarity and tf-idf weighting, using the 31 relevant football-related documents found in our control set as a seed set. It shows the recall and precision achieved when documents similar to one of the 31 seed documents are selected for various threshold values. When compared to Tables 3.2 and 3.3, Table 3.4 shows, for this particular example and this particular similarity measure, somewhat inferior results to those achieved by the well-crafted search terms or relevance ranking. In this example, for a review effort of 18,092 documents, cosine similarity achieves 49.1 percent recall and 21.2 percent precision—substantially inferior to the recall and precision results shown for the 18,092 Hits and # Top-Ranked Documents in Tables 3.2 and 3.3, respectively.[17]

TABLE 3.4 Similarity Search Using 31 Control-Set Seed Documents: Recall and Precision at Various Cut-Off Points

# Top-Ranked Documents	Recall	Precision
4,319	30.2%	54.5%
18,092	49.1%	21.2%
35,444	61.8%	13.6%
42,860	65.8%	11.9%
66,194	74.2%	8.7%
95,545	80.0%	6.5%

Classifiers

According to our Glossary, a classifier is "[a]n Algorithm that Labels items as to whether or not they have a particular property. . . ."[18] Within the context of e-discovery, classifiers are algorithms that yield a determination of relevant or nonrelevant. Classifiers may be constructed either manually or automatically.

A rule base is a manually (but systematically) constructed set of rules that is subsequently applied automatically to rank or classify documents as to their relevance. Thus, a rule base is simply a manually constructed classifier. In contrast to a rule base, a learned classifier is constructed automatically by a supervised machine-learning algorithm. The systematic construction of classifiers from training documents is the key factor that distinguishes TAR from search and analysis.

Whether manually constructed or learned, there are many different kinds of classifiers. A Boolean query could be used to form a simple classifier by deeming the "hits" to be relevant and the "misses" to be nonrelevant, or vice versa. Similarly, a classifier could be derived from a relevance ranking by deeming the top (or bottom) *k* results to be relevant, and the rest to be nonrelevant, for some cut-off value, *k*. A classifier might also be derived from a similarity search by deeming all documents with similarity *s* or greater to a document in the seed set to be relevant, and the rest to be nonrelevant, or vice versa.

A particularly simple but effective type of classifier is a linear classifier, which is simply a score for each term (or more generally, "feature") that may occur in a document, with positive scores indicating relevance, and negative scores indicating nonrelevance. The score of the document is simply the sum of the scores for the terms or features it contains, and the document is classified as relevant if its score exceeds some threshold, *c*, and nonrelevant if its score is less than *c*. Linear classifiers may be constructed by hand, in which case they are rule bases, or by supervised machine-learning algorithms, such as support vector machines (SVMs), logistic regression (LR), or naïve Bayes (NB).[19] Some of these classifiers are transparent, in that the mechanics of their operation—but not their effectiveness— is exposed; most are opaque, either because of their complexity, or because they rely on sophisticated pattern matching, parsing, or inference algorithms.

Rule-Based Methods for TAR

The construction of an effective rule-based TAR system is an expert-intensive process, relying on one or more domain experts (also known as subject-matter experts, or SMEs), as well as one or more rules-construction expert(s) (also known as knowledge engineers, and typically persons with expertise in linguistics, statistics, and/or computer science). While it may be easy to understand operationally how simple rule bases—notably flowcharts and decision trees—work, it is not easy to predict their effectiveness at discriminating between relevant and nonrelevant documents.

The rule-based approach determined to be effective in our JOLT article relied on extensive collaboration among a team of subject-matter experts, linguists, statisticians, and document reviewers, to construct and validate a complex set of rules in the form of Boolean expressions. The rules-construction experts formulated a series of Boolean queries, and reviewed examples of hits and misses for each query. Where the hits were found to contain too many nonrelevant documents, supplemental queries were constructed to remove these false-positive documents; where the misses were found to contain too many relevant documents, supplemental queries were constructed to identify the false-negative documents. This process was continued until the overall set of queries yielded acceptable recall and precision, as estimated using a control set.

There is some debate in the legal field as to whether Boolean search constitutes TAR. As previously illustrated, a classifier can consist of Boolean expressions. This is not to say that any use of a Boolean query is TAR—it may constitute TAR if the method of construction is systematic and is based on the iterative examination of exemplar documents using a control set. In any event, the label "TAR" does not, in itself, imply that the classifier is effective.

A number of do-it-yourself linguistic tools are available in the market for rule-base construction. One simple method relies on the examination of the vocabulary contained in the document collection —an exhaustive index of the words it contains, with stop-words eliminated— and asks the searcher to identify those words that appear most relevant to the subject matter of interest, and those that appear unlikely to be relevant. Another asks the searcher to highlight terms or phrases of interest. Unless followed up by an iterative query-refinement process, and a method to gauge progress by examining its effect on the documents in the collection, such approaches do not fit our definition of TAR.

Other do-it-yourself rule bases employ different kinds of classifiers, such as patterns or grammars. At the time of this writing, we are unaware of any scientific study demonstrating the effectiveness of any of these methods.

Similarity Search for TAR

Some of the most widely adopted TAR tools on the market rely on similarity search. Although commonly associated with supervised machine-learning methods, TAR methods based on similarity search closely resemble rule-based methods. The seed set represents a set of rules that determine which documents to deem relevant (due to their similarity to a relevant seed document) and which documents to deem nonrelevant (due to their dissimilarity to all relevant seed documents and/or their similarity to a nonrelevant seed document). Some TAR systems based on similarity search construct only a partial classifier, which is unable to classify certain gray-area documents as either relevant or nonrelevant.

As with untested search terms in Boolean rule-base construction methods, an initial seed set chosen intuitively (or at random) is unlikely to yield an effective classifier. It is necessary to apply the classifier to example documents, and, where the reviewer disagrees with the classifier's result, amend the seed set, either by adding new documents to the seed set, or by deleting or changing the coding of the seed document(s) responsible for the incorrect classification. This iterative process of sampling and revision continues until the classifier yields sufficient recall and precision.

While the mechanism of these similarity search tools is easily understood, as we have previously stated, the documents in the seed set—just like a list of search terms or Boolean queries—offer little insight as to the classifier's effectiveness.

Supervised Machine Learning for TAR

A number of TAR tools on the market—often referred to as "predictive coding" in e-discovery circles—employ an approach known in the information retrieval community as supervised learning, in which a machine-learning algorithm infers how to distinguish between relevant and nonrelevant documents, based on exemplar documents, each of which has been labeled by a subject-matter expert as relevant or nonrelevant. The entire set of exemplar documents is properly known as the "training set," although it is often incorrectly referred to as the "seed set." Typically, the learning method identifies combinations of features from the documents that distinguish relevance from nonrelevance; in many systems, the features consist of the words contained in the documents; in other systems, the features may include word fragments, phrases, concept clusters, punctuation, emoticons, or metadata.

Many supervised learning algorithms have been proposed. Among the most effective are support vector machines, logistic regression, bagging, boosting, random forests, and k-nearest neighbor (k-NN).[20] Common, but generally less effective, methods include naïve Bayes (colloquially known as "Bayesian"), nearest neighbor (NN, or 1-NN, which is essentially similarity search), and Rocchio's vector-space method.[21]

It is important to distinguish *supervised* learning methods from *unsupervised* learning methods.

Unsupervised methods do not use a training set, or any other human input as to what constitutes relevance. Such methods, which automatically group documents or document features without human oversight, include clustering, latent semantic indexing or analysis (LSI or LSA), and probabilistic latent semantic indexing or analysis (PLSI or PLSA).[22] These methods are not TAR tools in their own right, but may be used as a component of similarity search, or to derive features (e.g., concept clusters) for use in a supervised machine-learning method.

We have recently taxonified the various supervised machine-learning TAR protocols in use today into three major categories, referred to as "simple passive learning" (SPL), "simple active learning" (SAL), and "continuous active learning" (CAL).[23] SPL represents the most basic application of supervised machine learning. In SPL, all of the training documents are selected either at random, by the human operator of the TAR system, or through a combination of both methods. SAL extends SPL to allow the learning algorithm to identify exemplar documents to be reviewed, coded, and added to the training set. CAL repurposes the role of the classifier in supervised learning, abandoning the objective of creating, once and for all, the best possible classifier, in favor of constructing a series of disposable classifiers—each with the sole purpose of identifying more relevant documents for review—and continuing to construct classifiers— each trained on all documents reviewed to date—until substantially all relevant documents in the collection have been reviewed. These core protocols are compared and contrasted in the following sections and are set forth in Table 3.7.

Active Versus Passive Machine-Learning Methods

In taxonifying supervised machine-learning protocols for TAR, it is important to distinguish between the roles of teacher and learner. The *teacher* is the human operator of the TAR system, while the *learner* is the machine-learning algorithm. The term "passive learning" means that the learner (i.e., the algorithm) is passive in the selection of training examples; it plays no part in that selection and uses for training only those exemplar documents selected by the teacher, or through random selection. By contrast, the term "active learning" means that the learner (i.e., the algorithm) actively selects some—usually most— of the documents from which it will learn. These documents are coded by the teacher and then fed back to the algorithm for further training. In other words, *passive versus active learning is assessed from the perspective of the learner*—the algorithm—and its level of involvement in selecting the documents it will be given for training purposes; the algorithm is either an active or a passive participant in the selection process.

Passive learning must be distinguished from passive teaching. In passive teaching, the teacher plays no role in selecting the training examples for the algorithm; instead they are selected either at random, by the learner, or through a combination of both methods. By contrast, the term "active teaching" means that the teacher selects some—or most—of the documents used for training using her judgment, for example, by selecting training examples identified during witness interviews, through ad-hoc search methods, from prior productions, and even through the creation of "synthetic documents" that would be of interest, if they were to be found in the collection.

One principal factor distinguishing different TAR protocols is how the training documents are chosen: by the teacher, by the learner, at random, or through some combination of these approaches. While some controversy persists as to which method of selecting training examples is preferable, the question is amenable to empirical evaluation.[24]

The argument for exclusively randomly selected training examples appears to derive from several sources:

- The fact that much theoretical and empirical research on supervised machine learning assumes that the training set is a random sample of the collection;
- The conviction—possibly owing to experience with similarity search—that the training documents *must* represent all the different kinds of potentially relevant documents in the collection, and the mistaken assumption that random sampling is likely to achieve this;
- The erroneous belief—derived from the confusion between control and training sets—that using a random training set of a particular size will guarantee a particular level of classifier effectiveness; and,
- Distrust of reliance on the teacher's skill, knowledge, and goodwill in choosing appropriate training examples, and fear that any "bias" in selection will be transferred to, if not amplified by, the learner.

The argument for active teaching (whether or not augmented by random training and/or active learning) derives from the fact that the teacher is familiar with the subject matter, and therefore best positioned to find a set of representative documents from which the learner can deduce the best classifier, so that no obvious category of responsive document will be overlooked. Current research suggests, that such subject-matter expertise may not be necessary for certain active learning methods, for which a single relevant document may be sufficient to kick-start the TAR process.[25]

The argument for active learning (whether or not augmented by random training and/or active teaching) derives from the fact that the learning algorithm is best positioned to identify the documents from which it would learn most, akin to a small child repeatedly pointing and asking, "Is that a relevant document?" "What about this one?" "And, that one?"

Simple Versus Continuous Machine-Learning Methods

The second principal factor distinguishing supervised machine-learning protocols is: When should training stop? For simple passive learning and simple active learning, the answer is, "When the classifier is good enough," for some definition of "good enough," which is typically measured in terms of the recall, precision, or F_1 of the classifier, and often referred to as the "stabilization" point. When the stabilization point has been reached, and it is determined that further training will not improve the classifier, the training phase ceases and the review phase begins. The learned classifier does not continue to improve as more documents are reviewed.

For continuous active learning, the answer to the question, "When should training stop?" is, "When enough relevant documents have been found," for some definition of "enough relevant documents," typically measured by a precipitous drop-off in precision, and subsequently, by calculating recall at the end of the review process. For CAL, there is no distinction between the training and review phases. The learned classifier continues to improve as more and more documents are reviewed.

With all TAR protocols, the definition of "enough"—whether measured by a "good-enough" classifier or by identifying "enough" relevant documents—is based on proportionality considerations: How much could the result be improved, in terms of the value of the relevant information in any new documents found, relative to the additional review effort required to find that information? Over and above imprecision in quantifying the value of the information, and the challenge of measuring it with sufficient accuracy, such a determination requires clairvoyance to determine the future consequences of stopping or continuing training. This is currently one of the biggest challenges for all TAR protocols.

While a standard definition of "enough" has yet to be established, some commentary has argued—and some case law has accepted—a statistical recall estimate of at least 75 percent, with a margin of error of ±5 percent, and 95 percent confidence level, as indicating that "enough relevant documents" have been identified.

Core Supervised Machine-Learning Protocols Used for TAR

The machine-learning approach found to be effective in our JOLT article used a combination of active teaching, active learning, and continuous learning. Initial examples for review and training were the top-ranked hits (based on relevance ranking) of hundreds of simple keyword searches, while subsequent examples were those given the highest score by a logistic regression algorithm, or found through supplemental keyword searches. Review and training continued until an insubstantial fraction of the top-scoring documents that had not yet been reviewed were relevant; in other words, the precision of the top-ranked documents was low, suggesting that there were few relevant documents left to be found.

The protocol just described is an example of continuous active learning. The essential characteristic of CAL is that, after the initial seed set, which may be judgmentally selected by the human teacher, throughout the remainder of the review, it is the learning algorithm that repeatedly suggests additional documents for review. These documents are then coded by the teacher and used for training the learning algorithm. Typically, the selected documents are those that the learning algorithm is most confident are likely to be relevant, hence the name "relevance feedback." Review and training continue in iterative cycles until substantially all relevant documents have been identified. Documents never identified by the process are presumed to be non-relevant, following appropriate sampling and other validation procedures. The use of keyword searches to find documents both at the outset and throughout the TAR process (i.e., active teaching), though beneficial, is not an essential aspect of the particular CAL implementation studied in our JOLT article; nor is the use of logistic regression for the learning algorithm, and certain other design choices.

The results of applying CAL to identify the relevant documents in our fantasy football example are shown in Table 3.5. This CAL implementation[26] uses a single synthetic seed document, consisting only of the request for production for Topic 207, set forth earlier in this chapter; all other training examples were selected by the learner. A comparison of Tables 3.2, 3.3, and 3.4 with Table 3.5 shows that, for any given level of review effort, CAL achieves substantially higher recall and higher precision than the carefully crafted search terms, relevance ranking using these search terms, and similarity search using as a seed set the 31 relevant documents found in the control set. When 18,092 documents are reviewed, CAL achieves 95.5 percent recall and 41.2 percent precision, as compared to 67.0 percent recall and 28.9 percent precision achieved by the best of the other methods previously described in this chapter.

TABLE 3.5 Recall as a Function of Review Effort for the CAL Implementation Distributed to the TREC 2015 Total Recall Track Participants

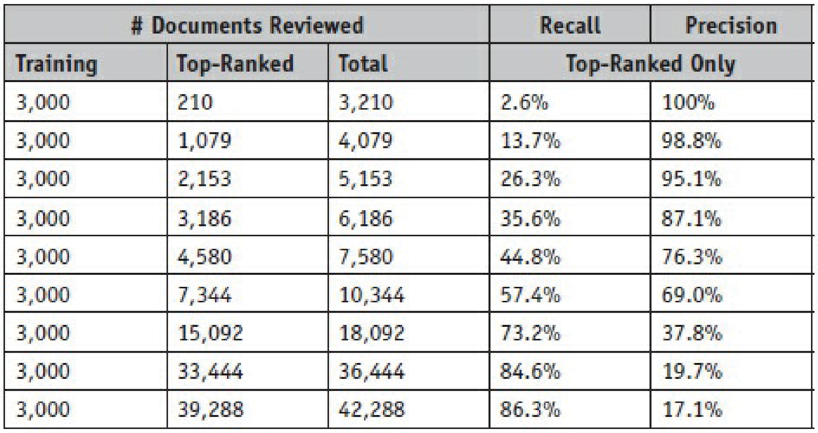
# Documents Reviewed	Recall	Precision
3,210	40.0%	97.2%
4,079	50.0%	95.6%
5,153	60.0%	90.8%
6,186	70.0%	88.3%
7,580	80.0%	82.3%
10,344	90.0%	67.9%
18,092	95.5%	41.2%

At the time of this writing, CAL has yet to be widely adopted within the e-discovery community, although its use is gradually increasing. Most commercial TAR offerings still employ either simple passive learning or simple active learning.

The defining characteristic of SPL is that the learning algorithm plays no role in selecting the training examples. Examples are selected either at random, through active teaching (i.e., judgmental selection by the teacher), or through a combination of both. Once reviewed and coded, the examples are used to train the learning algorithm. The effectiveness of the training is evaluated with respect to a sample of documents in the collection (typically, the control set), and, if the effectiveness is found to be satisfactory (a point commonly referred to as stabilization), training ceases and the resulting classifier is applied to the entire collection to identify a "review set" of presumed-relevant documents. Documents not in the review set are presumed to be non-relevant after sampling or other validation processes.

Table 3.6 shows the recall and precision achieved for the fantasy football example for SPL using, as a training set, the same 3,000 randomly selected documents that we previously used as a control set, and for identifying seed documents for the similarity search described earlier in the chapter. The SPL review effort (Total, shown in the third column) has two components: first, review of the training set (Training, shown in the first column) and then, the review set (Top Ranked, shown in the second column). For a total review effort of 18,092 documents, SPL achieves 73.2 percent recall and 37.8 percent precision, substantially better than the previously described search methods, but worse than CAL.

TABLE 3.6 Review Effort, Precision, and Recall for SPL Using 3,000 Randomly Selected Training Documents



# Documents Reviewed			Recall	Precision
Training	Top-Ranked	Total	Top-Ranked Only	
3,000	210	3,210	2.6%	100%
3,000	1,079	4,079	13.7%	98.8%
3,000	2,153	5,153	26.3%	95.1%
3,000	3,186	6,186	35.6%	87.1%
3,000	4,580	7,580	44.8%	76.3%
3,000	7,344	10,344	57.4%	69.0%
3,000	15,092	18,092	73.2%	37.8%
3,000	33,444	36,444	84.6%	19.7%
3,000	39,288	42,288	86.3%	17.1%

SPL achieves high recall with less review effort than a carefully crafted keyword search, keyword-based relevance ranking, and similarity search, but requires considerably greater effort than CAL to achieve the same recall. Notably, very few responsive documents are found during the initial effort to review the 3,000 training documents. This initially unproductive training effort may serve as a disincentive to the use of SPL.

SAL falls somewhere between CAL and SPL. Like CAL, SAL employs an active learning strategy in which, after using some examples supplied either by the teacher or through random selection, the learner then selects the remaining training examples. However, the SAL learner typically employs an “uncertainty sampling” approach, selecting documents about which it is least certain, and from which it can therefore learn the most. Like SPL, SAL employs separate training and review phases, where the classifier is fixed at the end of the training phase. The net effect is that SAL shares with SPL a generally unproductive training phase (in the sense that a low proportion of relevant documents are initially identified) and the need to determine when the classifier is “good enough” (i.e., a stabilization point). When this determination is accurately made, SAL can achieve similar recall and precision to CAL.

TABLE 3.7 Comparing CAL, SAL, and SPL Protocols for TAR

CAL Protocol	SAL Protocol	SPL Protocol
STEP 1: Choose a seed set using judgmental sampling (e.g., attorney search, known relevant documents, synthetic documents, etc.). **STEP 2:** Review and code the documents in the seed set. **STEP 3:** Use the machine-learning algorithm to suggest the next most-likely responsive documents for review (i.e., relevance feedback). **STEP 4:** Review and code the newly suggested documents and add them to the training set. **STEP 5:** Repeat steps 3 and 4 above until substantially all relevant documents have been reviewed (i.e., precision drops off precipitously). **STEP 6:** Validate the TAR process.	**STEP 1**: Create a random control set. **STEP 2:** Review and code the documents in the control set. **STEP 3:** Choose a seed set using random sampling, judgmental sampling (e.g., attorney search, known relevant documents, synthetic documents, etc.), or a combination of both. **STEP 4:** Review and code the documents in the seed set. **STEP 5:** Use the machine-learning algorithm to suggest those documents from which the algorithm will learn the most (i.e., uncertainty sampling). **STEP 6:** Review and code the newly suggested documents and add them to the training set. **STEP 7:** Repeat steps 5 and 6 above until training is deemed to be sufficient and "stabilization" occurs. **STEP 8:** Run the machine-learning algorithm for the final time to categorize or rank all documents in the collection. **STEP 9:** Review the documents categorized as "relevant," or ranked above some "cut-off" score. **STEP 10:** Validate the TAR process.	**STEP 1**: Choose a seed set using random sampling, judgmental sampling (e.g., attorney search, known relevant documents, synthetic documents, etc.), or a combination of both. **STEP 2:** Review and code the documents in the seed set. **STEP 3:** Run the machine-learning algorithm and evaluate the effectiveness of training thus far. **STEP 4:** If the result is insufficient, repeat the steps above with an augmented training set. **STEP 5:** When training is deemed to be sufficient, run the machine-learning algorithm for the final time to categorize or rank all documents in the collection. **STEP 6:** Review the documents categorized as "relevant," or ranked above some "cut-off" score. **STEP 7:** Validate the TAR process.

Other Aspects of the Electronic Discovery Process That May Impact TAR

Any implementation of TAR will necessarily occasion certain choices regarding the identification, collection, and culling of the documents subject to search and review; staffing and other workflow decisions related to the specific tool and protocol to be applied; and the selection and implementation of quality-control and validation processes. While these activities are ancillary to TAR per se, they are important aspects of the review process, and can exert a significant impact on the quality and success of a TAR effort. Many of these important issues are addressed in other chapters of this book.

[1] Maura R. Grossman & Gordon V. Cormack, *Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review*, 17 RICH. J.L. & TECH. 11 (2011), http://jolt.richmond.edu/v17i3/article11.pdf.

[2] Maura R. Grossman & Gordon V. Cormack, *The Grossman-Cormack Glossary of Technology-Assisted Review*, with Foreword by John M. Facciola, U.S. Magistrate Judge, 7 FED. COURTS. L. REV. 1, 32 (2013), http://www.fclr.org/articles/html/2010/grossman.pdf.

[3] Bruce Hedin, Stephen Tomlinson, Jason R. Baron, & Douglas W. Oard, *Overview of the TREC* 2009 *Legal Track*, *in* NIST S PECIAL P UBLICATIONS: SP 500-278, THE EIGHTEENTH TEXT RETRIEVAL CONFERENCE (TREC 2009) PROCEEDINGS, 6 (2009), http://trec.nist.gov/pubs/trec18/papers/LEGAL09.OVERVIEW.pdf; Gordon V. Cormack, Maura R. Grossman, Bruce Hedin, & Douglas W. Oard, *Overview of the TREC* 2010 *Legal Track*, *in* NIST SPECIAL PUBLICATION: SP 500-294, THE NINETEENTH TEXT RETRIEVAL CONFERENCE (TREC 2010) PROCEEDINGS 2 (2010), http://trec.nist.gov/pubs/trec19/papers/LEGAL10.OVERVIEW.pdf; Adam Roegiest, Gordon V. Cormack, Maura R. Grossman, & Charles L. A. Clarke, TREC 2015 Total Recall Track, http://trec-total-recall.org. The Text REtrieval Conference (TREC) is an annual workshop sponsored by the National Institute of Standards and Technology (NIST), the purpose of which is to support research in the information retrieval community by providing the infrastructure necessary for large-scale evaluation of text-retrieval methodologies. The Total Recall Track is part of TREC 2015, *see* http://trec.nist.gov.

[4] Roegiest et al., *supra* note 3.

[5] Blogger Ralph Losey has compared this approach to the child's game of Go Fish. Ralph C. Losey, *Child's Game of "Go Fish" is a Poor Model for e-Discovery Search*, E-DISCOVERY TEAM BLOG (Oct. 4, 2009), http://e-discoveryteam.com/2009/10/04/childs-game-of-go-fish-is-a-poor-model-for-e-discovery-search/.

[6] David C. Blair & M.E. Maron, *An Evaluation of Retrieval Effectiveness for a Full-Text Document-Retrieval System*, 28 COMMC'NS ACM 289 (1985).

[7] Grossman & Cormack, *supra* note 2, at 26 ("Prevalence: The fraction of Documents in a Population that are Relevant to an Information Need. Also referred to as Richness or Yield.").

[8] The validity of the repeated use of control sets for the purposes of statistical estimation is beyond the scope of this chapter, but is addressed in William Webber, Mossaab Bagdouri, David D. Lewis, & Douglas W. Oard, *Sequential Testing in Classifier Evaluation Yields Biased Estimates of Effectiveness, in* PROCEEDINGS OF THE 36TH INTERNATIONAL ACM SIGIR CONFERENCE ON RESEARCH AND DEVELOPMENT IN INFORMATION RETRIEVAL (SIGIR '13), 933–36 (2013), http://dl.acm.org/citation.cfm?id=2484159.

[9] *See* STEFAN BÜTTCHER, CHARLES L.A. CLARKE, & GORDON V. CORMACK, INFORMATION RETRIEVAL: IMPLEMENTING AND EVALUATING SEARCH ENGINES (MIT Press 2010), ch. 10, at 338.

[10] We applied the TWFS method described in Section 4.2, at p. 4, of D. Sculley & Gordon V. Cormack, *Going Mini: Extreme Lightweight Spam Filters, in* PROCEEDINGS OF THE SIXTH CONFERENCE ON EMAIL AND ANTI-SPAM (CEAS '09) (2009), http://ceas.cc/2009/papers/ceas2009-paper-47.pdf.

[11] *See* Eero Sormunen, *Extensions to the STAIRS Study—Empirical Evidence for the Hypothesized Ineffectiveness of Boolean Queries in Large Full-Text Databases*, 4 INFO. RETRIEVAL J. 257 (2001), http://www.sis.uta.fi/infim/julkaisut/fire/INRT87-JKwithFigs1.pdf.

[12] Grossman & Cormack, *supra* note 2, at 28.

[13] *See* STEFAN BÜTTCHER ET AL., *supra* note 9, ch. 5, at 138–41 & ch. 8, at 258–81.

[14] *See* Sculley & Cormack, *supra* note 10.

[15] Losey, *supra* note 5.

[16] *See generally* STEFAN BÜTTCHER ET AL., *supra* note 9, ch. 3 & 4, at 84–136.

[17] It is important to note that the results presented in Tables 3.2 through Table 3.6 are illustrative examples, only. While the results are typical of those we have observed, they do not show that any class of methods is superior to, or inferior to, any other class of methods in all circumstances. Such questions are best addressed through controlled scientific studies. *See, e. g.*, Cormack & Grossman *infra* note 23.

[18] Grossman & Cormack, *supra* note 2, at 11.

[19] *See generally* Büttcher et al., *supra* note 9, ch. 10 & 11, at 310–404.

[20] *See generally id*.

[21] *See generally id*.

[22] *See* Grossman & Cormack, *supra* note 2, at 11, 22, 26.

[23] Gordon V. Cormack & Maura R. Grossman, *Evaluation of Machine-Learning Protocols for Technology-Assisted Review in Electronic Discovery, in* PROCEEDINGS OF THE 37TH INTERNATIONAL ACM SIGIR CONFERENCE ON RESEARCH AND DEVELOPMENT IN INFORMATION RETRIEVAL (SIGIR '14), 153–62 (2014), http://dx.doi.org/10.1145/2600428.2609601.

[24] *See generally id.*

[25] Gordon V. Cormack & Maura R. Grossman, *Autonomy and Reliability of Continuous Active Learning for Technology-Assisted Review*, arXiv:1504.06868 (2015), http://arxiv.org/abs/1504.06868.

[26] The particular implementation applied was the baseline model implementation (BMI) supplied to TREC 2015 Total Recall participants. *See* Roegiest et al., *supra* note 3.

Topic VI

Navigating the "Dark Web"

Materials Online Only

Topic VII

Ethical Implications of Cutting-Edge Technologies

Materials Online Only

Topic VIII

Panel Discussion: New Technologies and the Lawyer of the Future

Materials Online Only

Faculty Biographies

(Alphabetical Order)

John T. Bandler
Bandler Law Firm LLC
48 Wall Street, 11th Floor
New York, NY 10005
info@bandlergroup.com
(929) 265-2775

John Bandler founded Bandler Group LLC to provide consulting services and meet the needs of businesses and individuals in a variety of areas. John is experienced in the private sector and from over twenty years of government experience as a prosecutor, police officer, and Army officer. This experience can help corporations and individuals with the many issues that require expertise in cybersecurity, cybercrime, investigations, anti-money laundering, and more.

John possesses a broad background with many unique areas of expertise. John authored a book on cybersecurity and is a prolific writer. He speaks, teaches, and has provided subject matter expertise on topics including cybersecurity, physical security, cybercrime, virtual currency, anti-money laundering, and law. John has helped individuals, corporations, and financial institutions investigate cybercrime, improve their cybersecurity, and evaluate and improve their cybersecurity and information security programs.

In 2002, John was hired by the legendary Robert M. Morgenthau as an Assistant District Attorney at the New York County District Attorney's Office. For thirteen years he investigated and prosecuted a wide variety of cases ranging from global cybercrime and financial crime to violent street crime. Notably, together with a dedicated team, he was responsible for a ground breaking case, People v. Western Express International, Inc. et al. The investigation and prosecution uncovered the global trafficking of stolen hacked data, money laundering of digital currency criminal proceeds, and identity theft, and successfully prosecuted international cybercriminals and U.S. based identity thieves, which culminated in guilty verdicts after a lengthy trial in 2013.

In 1994 John graduated from the New York State Police Academy after the grueling six month training. He then served as a State Trooper in the New York State Police for eight years in one of the busiest stations in the state, providing full police services to the local community. While serving as a Trooper, he attended Pace University School of Law, where he graduated in 2002.

John graduated Hamilton College in 1992 with a major in Physics and a minor in Computer Science, and earned the Phi Betta Kappa key. John also earned his commission in the U.S. Army through the R.O.T.C. program, and went on to serve in the New York Army National Guard and U.S. Army Reserves, serving in Infantry and Military Intelligence Units.

John holds certifications in information security, privacy, anti-money laundering, fraud investigations, and information technology, including:

Certified Information Systems Security Professional (CISSP)
GIAC Certified Incident Handler (GCIH)
GIAC Certified Penetration Tester (GPEN)
GIAC Critical Controls Certification (GCCC)
Certified Information Privacy Professional (CIPP/US)
Certified Anti-Money Laundering Specialist (CAMS)
Certified Fraud Examiner (CFE)
CompTIA Cloud+
CompTIA Network +
CompTIA A+

Mark A. Berman, Esq.
Ganfer Shore Leeds & Zauderer, LLP
360 Lexington Avenue
14th Floor
New York, NY 10017
mberman@ganfershore.com
(212) 922-9250

Mark Berman is a partner in Ganfer Shore Leeds and Zauderer's litigation practice groups as well as in the firm's Cooperative and Condominium Housing Practice Group. He heads the firm's Discovery Counseling practice. He also co-heads the firm's Complex Title Insurance Litigation practice.

He has extensive experience in representing private and public companies, as well as partnerships and individuals, as plaintiffs and defendants, in complex commercial matters with an emphasis on real estate and securities disputes, electronic discovery conflicts, and complex title insurance issues.

Mr. Berman is experienced in all phases of litigation in both state and federal courts as well as in arbitral forums. He is a seasoned appellate attorney, having argued many cases before both the First and Second Departments. Mr. Berman is also a trained mediator.

Prior to joining Ganfer Shore Leeds and Zauderer, he was an associate in the litigation department at Skadden, Arps, Slate, Meagher & Flom LLP and clerked for United States Magistrate Judge Michael L. Orenstein for the Eastern District of New York.

Mr. Berman has written and lectured extensively on electronic discovery and social media issues before the American Bar Association, the New York State Bar Association and the New York State Judicial Institute, the First and Second Appellate Divisions of the New York Supreme Court. He has been appointed by the Chief Administrative Judge as a member of New York State E-Discovery Working Group advising the New York State Unified Court System.

Mr. Berman was Chair of the Commercial and Federal Litigation Section of the New York State Bar Association (NYSBA) for 2016-2017. He is currently chair of NYSBA's newly formed Committee on Technology and the Legal Profession.

Since 2005, Mr. Berman has authored a column in The New York Law Journal addressing electronic discovery under New York State law. Mr. Berman's articles have been quoted in both appellate and trial court decisions.

Mr. Berman is rated "AV" by Martindale-Hubbell, the highest level in professional excellence and ethics, and has been selected as a "New York Super Lawyer" annually since 2008.

EDUCATION

- Benjamin N. Cardozo School of Law (J.D. 1990), magna cum laude, Editor, Moot Court Board Order of the Barrister
- Columbia College (A.B. 1986)

Mayling C. Blanco, Esq.
Blank Rome LLP
405 Lexington Avenue
New York, NY 10174
mblanco@blankrome.com
(212) 885-5502

Mayling Blanco represents corporations and individuals in white collar defense, government investigations, and commercial litigation matters, notably concentrating her practice on the Foreign Corrupt Practices Act (“FCPA”) and corporate fraud, as well as matters implicating criminal tax exposure.

Mayling has conducted numerous domestic and international, multi-jurisdictional investigations for clients with ventures in Latin America, Asia, and Europe, and has represented her clients before the U.S. Department of Justice’s Criminal, Civil, and Tax Divisions. She regularly advises clients with respect to the development of anti-bribery plans and policies, audit findings, investigating potential violations, and anti-bribery inquiries arising from everyday business dealings. She also represents clients facing government investigation or seeking to conduct internal investigations.

Mayling also advises corporations and financial institutions, including their boards of directors and committees, in connection with corporate governance and compliance matters, particularly as they relate to internal investigations and mitigating civil regulatory and criminal exposure. She has significant experience assisting companies in efficiently responding to subpoenas, thereby minimizing any disruption to their business operations.

In litigation, Mayling has significant experience before various Federal District Courts, U.S. Tax Court, the Superior Court of New Jersey, the New Jersey Appellate Division, and the New Jersey Supreme Court, defending clients in white collar, tax, commercial, employment, and constitutional matters.

Prior to joining Blank Rome, Mayling served under the Honorable Mathias E. Rodriguez of the New Jersey Superior Court. During law school, she was a member of the Legislative Bureau Journal, a student fellow for the Immigration and Human Rights Clinic, and held executive positions with student organizations.

Admissions: New Jersey, New York , U.S. Tax Court

Education: Cornell University, BA; Seton Hall University School of Law, JD

NEW YORK STATE
BAR ASSOCIATION
NYSBA

Jerry Bui
U.S. Director of Forensics at Inventus
205 Lexington Avenue
19th Floor
New York, NY 10016
jbui@inventus.com
(212) 267-6600

Jerry Bui is the US Director of Forensics at Inventus LLC, a leading global eDiscovery services provider. Mr. Bui is responsible for all digital forensic services and evidence collection for investigation and litigation matters and has over 15 years of experience working for top-tier consulting firms and providing services in digital forensics, eDiscovery and data analytics. He has delivered both reactive and proactive solutions for large multinational corporations at global scale, specializing in automated risk assessments, risk-based audits, compliance monitoring, and investigative analytics. Mr. Bui's clients have spanned various industries, including pharmaceutical life sciences, medical device, healthcare, food safety, and technology.

Clifford R. Ennico, Esq.
Law Offices of Clifford R. Ennico
2490 Black Rock Turnpike
Suite # 354
Fairfield, CT 06825-2400
(203) 254 1727
crennico@gmail.com

Since 1996, Cliff Ennico has worked as a "general counsel" or "Wall Street lawyer" to hundreds of small businesses, entrepreneurs, franchise owners, self-employed professionals, not-for-profit entities, and other business clients throughout the northeastern United States. He graduated magna cum laude from Dartmouth College in 1975, and got his law degree from Vanderbilt University School of Law in 1980, where he was Articles Editor of the Vanderbilt Law Review.

During the 1980s, Cliff worked for a succession of law firms in New York City, where he specialized in corporate finance, venture capital and securities law. After a brief stint during the early 1990s as in-house counsel for General Electric Capital Corp., Cliff worked as a corporate/business lawyer for two Connecticut law firms before launching my own practice in 1996.

Cliff is admitted to practice law in New York and Connecticut, and am in good standing in both states. Cliff focuses on representing entrepreneurs, small business owners and self-employed professionals.

In addition to being a lawyer, Cliff also is:

- The author of several law books for West Group, a leading U.S. legal publisher, including a best-selling collection of legal forms called Forms for Small Business Entities.
- The author of Succeeding in Your Business™, a weekly business advice column that appears in dozens of newspapers nationwide as well as www.entrepreneur.com and other business-oriented Web sites.
- The former host of MoneyHunt, the popular PBS television show about entrepreneurs;
- An instructor for eBay University, where I advise entrepreneurs nationwide on legal and tax implications of buying and selling goods on eBay, the nation's leading internet auction site.

- The author of Small Business Survival Guide, a collection of useful tricks for dealing with the 12 biggest enemies you will face when you run your own business.
- The author of The eBay Seller's Tax and Legal Answer Book, the best - and ONLY - comprehensive guide to the legal and tax rules that apply when you're selling on eBay, the world's leading auction marketplace.
- A frequent contributor to Entrepreneur and other small business magazines, websites and blogs.
- A leading authority on entrepreneurship and small business management, giving talks to business groups nationwide.

Ignatius Grande
Berkeley Research Group, LLC
810 Seventh Avenue
New York, NY 10019
igrande@thinkbrg.com
(646) 809-8066

Ignatius Grande has advised clients on issues relating to information management, electronic discovery, and data privacy for more than fifteen years. With his legal and technical expertise, he bridges the gap that may exist between IT and legal/compliance departments. He has worked with both law firms and companies to guide them through the eDiscovery and forensic investigation process and has overseen the collection and production of data for several Hart–Scott–Rodino (HSR) second requests. He works with companies on data privacy practices and advises companies on compliance with European Union data-privacy laws, including the General Data Protection Regulation.

Mr. Grande has performed compliance risk assessments that addressed records retention, legal hold, and data-remediation issues. He often works to address complex information management issues, including the onboarding of new software and technologies and the privacy and security implications of Internet of Things (IoT) devices and sensors. He advises on information management practices and has helped draft and revise a variety of policies, including for Bring Your Own Device, Legal Hold, Records Retention, Social Media, and Mobile Device Governance.

Mr. Grande serves as co-chair of the Committee on New York State Bar Association's Litigation Section and teaches a course on eDiscovery at St. John's University School of Law.

Education

- Georgetown University Law Center, JD, 1999
- Yale University, BA, Political Science, 1996

Kevin J. Hart
Founder and CEO
Green Check Verified
5 Science Park
New Haven, CT 06511
khart@greencheckverified.com
(203) 671-2661

Mr. Hart is a career CEO specializing in digital transformation and enterprise company development. He has had multiple instances of successful scale and exit of technology companies.

Mr. Hart is an experienced, passionate, team-oriented leader that has held executive positions in venture backed technology companies.

Mr. Hart specializes in developing strategic plans coupled with organizational development with strong metric driven execution to achieve the next level of results.

Mr. Hart's diverse experience includes: Strategic planning, start-up and/or expanded business strategies, organizational development, sales organizations, and operational execution, all with exceptional executive relationships and BOD development.

NEW YORK STATE
BAR ASSOCIATION
NYSBA

Mary J. Hildebrand, Esq.
Lowenstein Sandler LLP
One Lowenstein Drive
Roseland, NJ 07068
mhildebrand@lowenstein.com
(973) 597-6308

Mary Hildebrand is a partner with Lowenstein Sandler LLP. For more than 30 years, Mary has drawn on her deep experience in privacy and data security, tech, and intellectual property to handle sophisticated technology deals from concept to conclusion.

Mary regularly serves as lead counsel to both public and private companies in complex commercial matters involving:

- Digital and social media
- Software
- Clean tech
- Renewable energy
- Public utilities
- Financial services
- Medical devices
- Entertainment
- E-commerce
- Transportation
- Universities
- Not-for-profit organizations

Additionally, she counsels startups on the transactions and foundational legal structures needed to launch their businesses.

As a leading intellectual property lawyer, Mary has achieved an enviable track record in commercializing, protecting, and managing intellectual property, technology, and database assets around the world. She is also a recognized authority on EU and U.S. data privacy and information security laws.

A highly regarded "top-notch," "hugely responsive," and "skilled, bright and knowledgeable" practitioner, Mary has been consistently recognized by Chambers USA (2009-2017) for her successful handling of complex transactions involving significant IP assets. Her clients commend her as "a phenomenal client manager" who gives "useful, pragmatic, practical advice."

Mary has served as a member of Lowenstein Sandler's board of directors and Strategic Planning Committee, as well as chair of the firm's Diversity and Inclusion Committee. She is a founder and co-chair of STRIDES, Advancing Women in Business, a firm-sponsored initiative that promotes visibility, leadership opportunities, and quality peer interaction for women in business.

Education

- Duke University School of Law (J.D. 1984)
- Union College of Union University (B.A. 1980), magna cum laude

Jason Lichter, Esq.
Director of Discovery Services
and Litigation Support
Pepper Hamilton LLP
620 Eighth Avenue, 37th Floor
New York, NY 10018-1405
lichterj@pepperlaw.com
(212) 808-2716

Jason Lichter is the director of discovery services and litigation support at Pepper Hamilton LLP. In this capacity, Mr. Lichter develops and implements strategies to ensure that the firm's clients receive the highest quality discovery and litigation support services in a cost-effective and defensible manner. Mr. Lichter advises colleagues and clients on how to leverage the latest technologies and e-discovery best practices to efficiently guide matters from initial document preservation and collection through to production and eventual presentation at trial. An area of particular emphasis is document review, for which Mr. Lichter applies well-developed protocols and procedures in staffing, training, project and vendor management, quality control, privilege review, knowledge transfer, and increasingly statistical analysis to promote efficiency, mitigate risk, and gather metrics for use in preparing accurate budget estimates.

Mr. Lichter has counseled clients and colleagues on such varied topics as the implementation of ediscovery readiness action plans, vendor requests for proposal, defensible approaches to preservation, forensic and reasonably tailored data collections, cloud-based and structured data considerations, efficient and cost-effective document filtering and review strategies (including technology-assisted review), and quality control techniques.

Mr. Lichter's strong technical background includes substantial computer science coursework while an undergraduate at Yale University, followed thereafter by work experience as a software engineer for Sapient, a leading technology services consultancy.

A litigator by training, Mr. Lichter has represented clients on a wide variety of complex commercial, labor and employment, and intellectual property disputes in state and federal courts and in a broad array of industries, including media, finance, insurance, maritime, hospitality, real estate, telecommunications and construction. Mr. Lichter also has achieved very favorable results for several pro bono clients. In 2009, he represented a former inmate as co-lead counsel in a week-long excessive-use-of-force trial in the Southern District of New York. Mr. Lichter obtained a complete plaintiff's verdict and a $750,000 damages award. Mr. Lichter also argued a criminal appeal before the New York Appellate Division, obtained a favorable settlement for a film editor seeking unpaid wages and editing credit on a Sundance awardwinning documentary, and recovered a domain name from a cybersquatter on behalf of Save the Children. In recognition of his dedication to providing pro bono services, Mr. Lichter received the Legal Aid Society Pro Bono Award in both 2006 and 2009 and was honored with the Association's 2008 Empire State Counsel Award. While at Harvard Law School, Mr. Lichter worked at the Berkman Center for Internet & Society, where he contributed to an amicus brief addressing novel copyright issues that was submitted at the request of the court.

EDUCATION
- J.D., Harvard Law School, 2004
- B.A., Cognitive Psychology, cum laude, Yale University, 2000

BAR ADMISSIONS
- New York, 2005 4 COURT ADMISSIONS
- U.S. District Court, Southern District of New York, 2005
- U.S. District Court, Eastern District of New York, 2005

Notes Pages

NYSBA

NYSBA

NYSBA