Business Track

Protecting Property (of the Estate) and (the Attorney/Client) Privilege in the Era of the Data Breach

Ira L. Herman, Moderator
Thompson & Knight LLP; New York

Michael L. Bernstein
Arnold & Porter LLP; Washington, D.C.

Kenneth M. Krys
KRyS Global; George Town, Grand Cayman, Cayman Islands

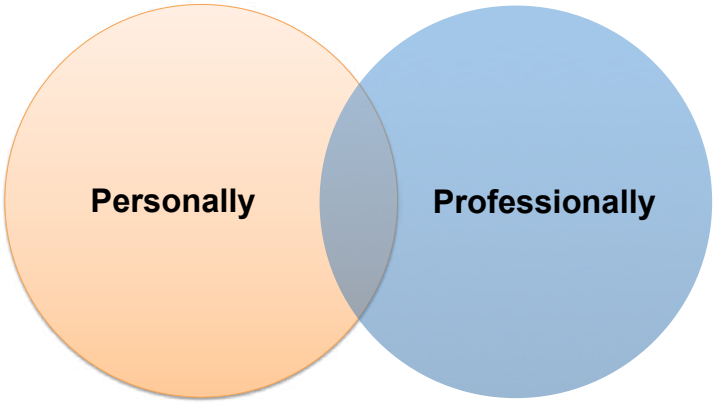
Monsita Lecaroz-Arribas
U.S. Trustee, Region 21; San Juan, P.R.

Protecting Client Confidences and Valuable Property of the Estate: Ethical Obligations and Best Data Security Practices

Thompson & Knight Impact

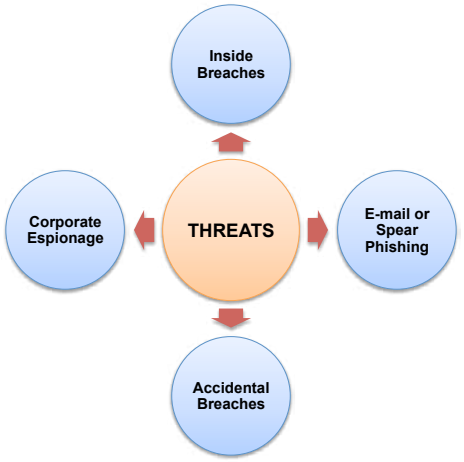
Presented by
Ira Herman

Why is this important?



Thompson & Knight Impact

What is the threat?



Thompson & Knight

Law Firms are especially Attractive Targets to Hackers

- This attractiveness is largely because of two compounding perceptions about law firms:
  - They are valuable targets
  - They are easy targets

Thompson & Knight

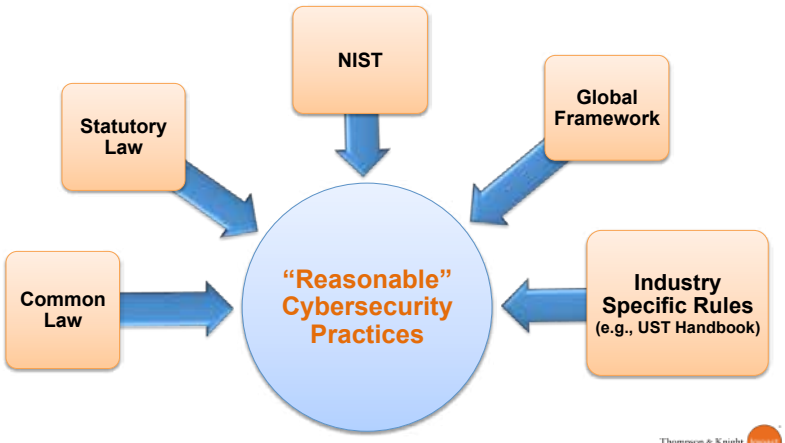
4

What should you do about it?

- Step 1 • Become aware of threats
- Step 2 • Analyze vulnerabilities
- Step 3 • Inventory data
- Step 4 • Understand the standard of care
- Step 5 • Meet the standard of care
- Step 6 • Develop and implement a security program

Thompson & Knight

What is the Standard of Care for Insuring Data Security?



Thompson & Knight

Ethical Obligations

- MRPC Rule 1.1
- MRPC Rule 1.6
- MRPC Rule 5.3 (Cmt. 3)

Thompson & Knight

Adapting to New Technologies

Professionals must inform themselves of the **risks of inadvertent or unauthorized disclosure** of client's cyber data and take reasonable and information-appropriate measures to reduce those risks

Thompson & Knight

8

Amended Model Rule 1.1

- "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."
  - Practically speaking, "[t]his provision will require lawyers to better understand any advances in technology that genuinely relate to competent performance of the lawyer's duties to a client."

Thompson & Knight

9

The Scope of the Duty of Confidentiality

- The duty of confidentiality is far broader than the narrow duty underpinning the attorney-client privilege
  - A lawyer owes a duty of care in protecting the confidences of a client, even those of a prospective client with whom no attorney-client relationship is formed. See ABA Comm. on Ethics and Professional Responsibility, Formal Op. No. 90-358, Sept. 13, 1990.
    - *United States v. Morrell-Corrada*, 343 F Supp 2nd 80, 88 (2004).

Thompson & Knight

10

Confidentiality

- In with limited exceptions, "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent."

Thompson & Knight

11

Extra Security Measures are Appropriate

- Compliance with minimum standards of any kind--including those delineated in ethics rules--should only be a starting point for effective cybersecurity practice"
  - The ABA Cybersecurity Handbook

Thompson & Knight

12

Supervising Third Parties

- A law firm's data security practices are only as strong as its weakest link
- Lawyers must make sure that law firm staff and external business partners understand necessary data security practices and the critical role all parties play in ensuring the protection of client information

Thompson & Knight

13

It's Not Just the People Anymore

- "To reflect the scope of the nonlawyer services now being provided outside of firms," Model Rule 5.3's commentary now references "cloud computing" as an example of modern outside help.

Thompson & Knight

14

Client Audits

- Clients are insisting that their lawyers take appropriate measures to protect proprietary or confidential information

Thompson & Knight

15

Limits of a Lawyer's Duties Under– Model Rule 5.3

- "A lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology," and "[w]hen it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard."
  - The New Hampshire Bar

Thompson & Knight

16

Data breaches – As a Liability Issue

- In most offshore jurisdictions liquidators are required to have professional indemnity insurance
- In the U.S. different types of date security insurance is being offered by insurers to professionals and their clients

Thompson & Knight

17

Property of the Estate

- Upon the filing of a bankruptcy petition, the bankruptcy estate is created from the Debtor's property
- Section 541 of the Bankruptcy Code defines what property is included in and excluded from a debtor's bankruptcy estate. See 11 U.S.C. § 541(a)-(f)

Thompson & Knight

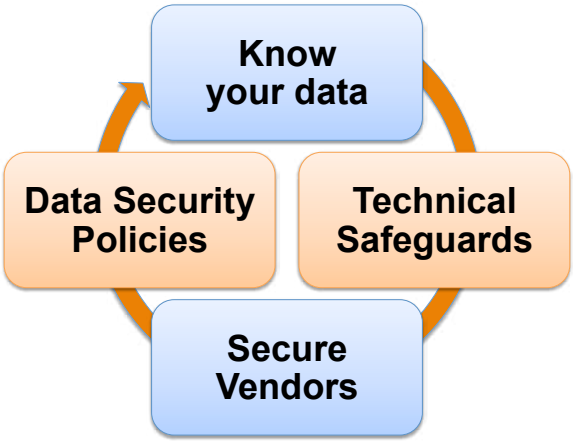
18

- The bankruptcy estate is the pool of assets that is subject to the jurisdiction of the bankruptcy court and from which creditors' claims are paid
- Electronically stored proprietary information can be the most valuable "property of the estate" in many bankruptcy cases

Thompson & Knight

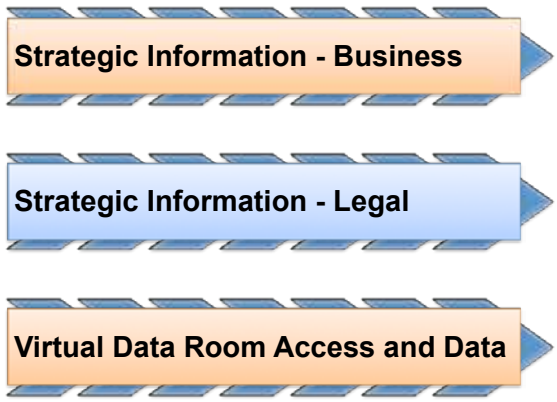
19

Protecting Valuable Client Information



Thompson & Knight

Risky Business for Bankruptcy Counsel



Thompson & Knight

21

PII

- Safeguarding personally identifiable information in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public
  - OMB memorandum Safeguarding Against and Responding to the Breach of Protecting Personally Identifiable Information (May 22, 2007)

Thompson & Knight

22

The United States Trustee's Handbook Requirements– Guidance for For All of Us

- **Chapter 7 trustees must comply with guidelines:**
  - **imposing specific restrictions on the use of wire transfers**
  - **requiring specific computer security measures**
  - **requiring trustees to develop and maintain a business interruption plan**
  - **requiring specific records security and retention policies, including individual case records and tax returns**
    - **The United States Trustee's Handbook for Chapter 7 Trustees (pages 5-15 to 5-21)**

Thompson & Knight

23

Steps in a Breach Response

Discovery & Reporting	• Identify the incident or potential incident. • Immediately report the incident or threat to the proper party.
Initial Response	• Secure and isolate affected systems to limit further data loss. • Preserve evidence. Convene the Incident Response Team in accordance with this Plan. • Know your role. Coordinate investigation and remediation.
Investigation	• Gather information on the incident. • Consider involving forensics team and outside counsel. • Analyze the cause of the incident and the affected systems. • Analyze legal requirements and liabilities going forward.
Remediation	• Comply with legal requirements including breach notification. • Remove known vulnerabilities; repairing systems. • Respond to third party inquiries. Consider contacting law enforcement.
Post-Incident Review	• Review analysis and notes regarding the incident. • Improve practices as necessary. • Improve policies as necessary.

Thompson & Knight

The Cayman and BVI Regimes

- Scheme of Arrangement
- Liquidation
- The Appointment of Fiduciaries and Their Respective Roles in the Process

Thompson & Knight

25

The U.S. Regime

- Chapter 7
  - Chapter 11
  - Chapter 15
  - The Appointment Fiduciaries and Their Respective Roles in the Process

Thompson & Knight

26

Conflicting Policy Imperatives

- Invariably, there will be conflicting standards of public policy when two or more jurisdictions are in play
  - How are disclosure and public policy driven matters best handled when more than a single jurisdiction is involved?

Thompson & Knight

27

Reporting Requirements, Disclosure and Due Process

- An Administrator's or Liquidator's reporting requirements are going to be different from those requirements in the U.S.
- Reports and filings that typically are public in U.S. cases may not be public in a non-U.S. jurisdictions
- Reports prepared by and administrator or liquidator may disclose more or less than is typical in the U.S. system

Thompson & Knight

28

Sealed Documents

- Recently, offshore courts have been making efforts to facilitate greater transparency in liquidations
- Liquidators are being pushed harder to explain why a document needs to be sealed and to set a deadline for unsealing sealed documents
- In a recent case, an offshore court entered a sealing order directing the liquidator to make an application, upon the closing of the liquidation, identifying documents to remain sealed and for how long

Thompson & Knight

29

Conflicting Disclosure/Discovery Regimes

- Transparency and secrecy issues – there may be unsolvable conflicts on shore and off shore
- For example, in certain situations, such as a sale of assets pursuant to section 363 of the U.S. Bankruptcy Code, disclosure requirements are stringent. The seller is required to disclose the status of any insider purchasers and relevant relationships between creditors, the debtor, etc.

Thompson & Knight

Differing or Conflicting Rules Governing Disclosure Electronic Communications

- What does one do when disclosure obligations/ restrictions on disclosure in a non-U.S. jurisdiction conflict with confidentiality rules at in the U.S.?
- In U.S. and non-U.S. jurisdictions can joint interest and confidentiality agreements be used successfully to shield shared information from discovery?

Thompson & Knight

31

Due Process Concerns

- "Notice and a hearing" in the U.S. versus lesser/ different due process/disclosure/notice requirements in other jurisdictions
- How do US courts view ex-parte orders issued in a non-US jurisdictions

Thompson & Knight

32

Breach & Breach Reporting

What is a breach?	How does a breach occur?	Now what?
• Hacking • Phishing • Malware • Theft • Misuse	• Motive • Opportunity • Weak security • Weak policies	• Respond quickly • Respond appropriately • Preserve evidence

Thompson & Knight

Client Counseling

- **The Chapter 7 Trustee or the DIP have fiduciary duties to creditors and other parties in interest**
- **As a lawyer – what are you client counseling obligations?**
- **Breach insurance**
- **Employee policies**
- **ESI preservation in contemplation of litigation**

Thompson & Knight

34

Index

Protecting Client Confidences and Valuable Property of the Estate: Ethical Obligations and Best Data Security Practices

Ira L. Herman, Mackenzie S. Wallace, & Craig C. Carpenter
Thompson & Knight LLP

American Bankruptcy Institute
2016 Caribbean Insolvency Institute
February 4-6, 2016
San Juan, Puerto Rico

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTORY AUTHORITIES

ADDITIONAL AUTHORITIES

Cybersecurity: What Attorneys (and their Clients) Need to Know.

Ira L. Herman, Mackenzie Wallace, & Craig Carpenter

Almost daily, there are reports of cyber attacks and misappropriation of data from companies of all sizes and across all industries. Evidence suggests that these threats are rising—the number of successful corporate cyber attacks doubled in the year 2012-2013, according to a fraud report released by Kroll investigators.[1] In the United States, for example, the government notified 3,000 companies in 2013 that they had been hacked. McAfee, *Net Losses – Estimating the Global Cost of Cybercrime*, Center for Strategic and International Studies (2014). McAfee estimates that the annual cost to the global economy from cybercrime is more than $400 billion. *Id.* The cost of cybercrime includes the effect of hundreds of millions of people having their personal information stolen in the US per year. *Id.* On average, companies spend more than $5 million to respond to each attack. The cost of cybercrime will continue to increase as more business functions move online and as more companies and consumers around the world connect to the Internet. *Id.* This explains why cybersecurity has become a top concern for corporate directors, officers and attorneys. These attacks are more sophisticated and persistent than ever. Threats include intellectual property theft and theft of sensitive information, loss of reputation and trust, loss of economic and competitive advantages, business disruption and liability to third parties.

Why Is This Important?

Data breaches are a problem for everyone; however, the risk is especially great for attorneys, who may have to be prepared to deal with this issue on both a personal and professional level.

Personally

As an individual you want to do everything that you can to protect your own identity and avoid the frustrations of identity theft that can result from a data breach. As an attorney, if you are a victim of a cyber attack the risk may be greater than just the individual annoyance to you, but you may potentially be liable for the breach of your client's sensitive, confidential information.

Professionally

As an attorney, you may have a duty to advise your clients on the cybersecurity risks that they face in their business operations and be prepared to assist them in the event of a breach and the ensuing litigation. In addition, lawyers may face an ethical duty stay abreast (at least at a high level) of data security issues.[2]

Attorneys must understand cyber threats to properly advise clients, and help clients understand the risks. Although attorneys are typically not the ultimate targets for hackers, hackers are often after the sensitive and valuable information that attorneys use, store, and transfer for clients. Attorneys often store extremely sensitive client information on their networks and computer systems (including trade secrets, financial information, personal family information, health information, and more), and they typically have this kind of information for multiple clients across a number of industries. Rather than trying to penetrate the sophisticated multi-national company to access or steal valuable data, hackers have found that a target's service providers (including attorneys) may be the path of least resistance to the company's crown jewels. This is the case because service providers often have less sophisticated defenses and are notoriously late at implementing the latest prophylactic technology and security programs. Hackers know the relationship of trust between attorneys and their clients, and although most cyber attacks still focus on corporations, roughly seven percent of all cyber attacks target the legal and consulting service industry. Because of the increased focus and vulnerability, sophisticated clients are increasingly demanding that their outside counsel meet certain cybersecurity standards.

What Is the Threat?

Hacking is no longer confined to viruses lurking on random websites or password cracking. Cybersecurity incidents include inside breaches, email phishing, spear phishing, accidental breaches (e.g., lost laptops and smart phones), and corporate espionage. The

[1] In a poll by Kroll of senior executives from large, global companies, Kroll found that 35% of firms had been victims of external hackers. The figure the previous year was 18%, according to a report by the Financial Times.

[2] The ABA Model Rules and at least 18 states have adopted duties of "technology competence," which could be read to include awareness of data security. See Section I, below.

insider threat is possibly the most significant data protection risk that companies face. Technology has made it easy for a disgruntled employee to alter or steal proprietary company data, accounting for one in five attacks across all industries. The consequences of such events can be devastating and often more costly than those by outside hackers. The insider threat is difficult to predict and prevent as it does not take a veteran hacker or a computer scientist to drag and drop files to a USB thumb drive or email documents from a work computer to a personal email account. The strength of a company's firewall and intrusion detection system does not help when the attack comes from within.

The demand for 24/7 access and mobility has also added concerns about unintentional employee data loss. With the advent of "Bring Your Own Device" mobility and mobile computing policies, more companies and firms are entrusting sensitive information to employee devices. This trend can boost efficiencies, but it can also create easier access for hackers. The attack may not even be intentional: innocent mistakes such as a laptop lost at the airport or a smart phone left in a taxi can lead to data breaches.

The digital attacks that attorneys and their clients face are also becoming more sophisticated, as cybercriminals use well-planned and targeted attacks, to exploit known vulnerabilities in a company's systems and use custom malware not identified by most over-the-counter anti-virus programs. These attacks tend to employ social engineering tactics to trick a target into opening an email containing a link to a malicious attachment or website by including personal information about the target in the email. The attacks often use information found on social media accounts and are sent under the guise of a close friend seeking help or an update from that person's bank to make it look trustworthy and legitimate.

The threat is particularly concerning for attorneys that create, manage or store financial, personal identity, or health-related information. This includes financial information, tax information, digital assets, social security numbers, trade secrets, and more. Hackers can use this information to impact a company's competitive advantage, steal critical information, or steal an individual's identity.

What Should You Do About It?

Given this increased threat landscape and the increased pressure on attorneys to raise their standards regarding security practices, what should attorneys do and how should they advise their clients?

It is impossible to guard against every possible cyber attack and no company or attorney is immune from this threat; however, there are important steps that can be taken to decrease the chance of becoming a victim and to decrease the impact and liability when a breach does occur. These steps include:

1. Become aware of current and evolving threats;
2. Analyze and understand your vulnerabilities;
3. Inventory the sensitive data you use, store, and transfer, and know where you store it on your systems;
4. Understand the applicable standard of care for the type of data you use, store, and transfer;
5. Take steps to meet the applicable standard of care; and
6. Develop and implement a security program appropriate for the type of data you keep and a data breach plan to manage security incidents.

This article will address relevant data protection standards as they apply to attorneys, steps to meet the applicable standards, and what to do in the event of a breach.

I. Standard of Care

Understanding the standard of care for sensitive client information is a critical first step to mitigating the liability an attorney may face in the event of a data breach.

A lack of regulatory engagement related to data security has left courts in an uncertain position about what steps attorneys or others should take to secure data and computer systems. The result has been a lack of clear definition regarding what constitutes a "standard of care" in the cybersecurity or data protection context. Currently, there are no comprehensive or base obligations as to data related to critical infrastructure in the United States. Instead, a complex patchwork of oftentimes-ambiguous state and federal regulations overlaying applicable common law doctrines exists. Scott Shackleford, et al., *Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable and International Cybersecurity Practices*, Maurer School of Law Indiana University, 50 Tex. Int'l L.J. 303 (2015).

Common Law in the United States

How are common law and statutory law shaping the standard of cybersecurity care in the United States?

Litigation involving a data breach may be brought under multiple liability theories and understanding the potential theories will help to identify the relevant standard of care.

Negligence is the most basic cause of action for a data breach. Avoiding liability for negligence generally requires conforming to a standard of conduct equivalent to that of another that would be considered "reasonable . . . under like circumstances." Restatement (Second) of Torts § 283 (1965). In cybersecurity law there is no explicit or overt "cybersecurity negligence" framework, although court opinions analyzing cybersecurity negligence demonstrate that a standard may be gradually emerging.

The court in *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, suggested that Sony's failure to employ industry cryptology standards was enough for plaintiffs to allege that Sony breached its duty to employ reasonable data security measures. No. 11md2258 AJB, 2014 WL 223677, at *2–3 (S.D. Cal. Jan. 21, 2014). Specifically, the court found, based on California and Massachusetts law, that because plaintiffs allege that they provided their personal information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect that information, including utilization of industry-standard encryption, the plaintiff sufficiently alleged a legal duty and corresponding breach. *Id.* at *12.

In any negligence action, the conduct of the party who suffered a data breach will be assessed against the duty of care owed by a reasonable person in similar circumstances. In these situations, the specific standard required depends on the character of the data or information. Factors considered include, the sensitivity of the stolen data, laws or regulations related to specific types of data, and common practices in the industry as to that data. Thus, attorneys should stay abreast of such regulations and common practices to ensure that both *personally*—in order to protect the sensitive client information they store—and *professionally*—to advise their clients—they understand and are meeting the standard of care.

In addition to suits for negligence, attorneys and corporate officers and directors may face liability arising from their fiduciary duties in the aftermath of a cyber attack. Because an attorney serves in a fiduciary role, he or she should pay extra cautions in managing sensitive data and responding to cyber threats. Two types of fiduciary duties that apply to corporate officers and directors have been: (1) the duty of loyalty, and (2) the duty of care. Fiduciary duties may be relevant to managing cyber attacks and shaping a cybersecurity duty of care. Related to the burgeoning duty in this context, liability may be found on the basis of a lack of good faith under the duty of loyalty if "(a) the [attorneys] utterly failed to implement any reporting or information system or controls; or (b) having implemented such a system or controls, consciously failed to monitor or oversee its operations[,] thus disabling themselves from being informed of risks or problems requiring their attention." *In re Citigroup Inc. S'holder Derivative Litig.*, 964 A.2d 106, 123 (Del. Ch. 2009).

Statutory Law in the United States

In addition to considering common law—including negligence and fiduciary duties—to help establish a standard of cybersecurity care, numerous state and federal statutes are also applicable. Several of the most applicable statutes and regulations related to establishing and shaping a standard of care for critical infrastructure organizations are summarized in Section II below.

In a recent case, the United States District Court for the District of New Jersey held that the Federal Trade Commission has the authority, pursuant to the statutory FTC Act, to bring enforcement actions against companies over allegedly lax data security practices. *Fed. Trade Comm. V. Wyndham Worldwide Corp.*, No. 13-1887, 2014 WL 1349019, at *6 (D.N.J. Apr. 7, 2014). This holding was largely affirmed by the Third Circuit earlier this year. *Fed. Trade Comm. V. Wyndham Worldwide Corp.*, No. 14-3514, (3d Cir. Aug. 24, 2015). The FTC sued Wyndham Worldwide Corporation in June 2012, alleging that the hotel chain did not do enough to protect consumers whose private information was accessed by hackers who breached the company's computer systems. The FTC claimed that Wyndham's actions amounted to a violation of Section 5 of the FTC Act, which allows the Commission to police unfair and deceptive trade practices. Wyndham challenged the FTC's data protection and enforcement authority, arguing that the FTC has no authority to take action against Wyndham

because the FTC has not published rules on what it requires from companies to protect against data breaches. In response to Wyndham's argument that the FTC does not explain what measures would be "reasonable," the court distinguished that the FTC described several data-security insufficiencies by Wyndham that could reasonably be believed to lead to data security breaches; however, the court's opinion still leaves uncertainty as to what data security practices companies should implement to be considered "reasonable."

As is evidenced above, no comprehensive cybersecurity standard of care has crystallized under common law or by statute, but the beginnings of a standard concerning negligence are emerging. Common law and statutory standards are considered incomplete and immature, opening the door for the National Institute for Standards and Technology ("NIST") Framework to have considerable impact on establishing a standard of care. Shackleford, et. al., *Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable and International Cybersecurity Practices* at 11.

Obama Administration & NIST

In February 2013, President Obama issued an executive order that, among other things, expanded public-private information sharing and tasked NIST with establishing a voluntary "Cybersecurity Framework" comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure. See *White House Press Sec'y, Executive Order on Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2013), available at http://www.whitehouse.gov/the-pressoffice/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity-0. The NIST Framework, *Framework for Improving Critical Infrastructure Cybersecurity*, was released in February 2014. National Institute for Standards & Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0 at 1 (2014). The Framework provides a voluntary procedure to map cybersecurity best practices and structure roadmaps for organizations to mitigate cyber risks. The Framework could help establish a baseline "standard of cybersecurity care" that could define legal liability for critical infrastructure organizations prior to and following cyber attacks.

The Framework provides steps for entities to evaluate their current cybersecurity posture. The substance of the Cybersecurity Framework is composed of three parts: (1) The Framework Core, (2) The Framework Implementation Tiers, and (3) The Framework Profile.

The Framework Core "provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes." Shackleford, et. al., *Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable and International Cybersecurity Practices* at 30. The Framework Core is an organizational map of industry-recognized cybersecurity practices that are helpful in managing cybersecurity risk and provides unified terminology for organizations to understand successful cybersecurity practice outcomes.

After mapping common cybersecurity activities and the various standards and practices employed to conduct these activities, the Framework provides a method for an organization to understand the degree to which its cybersecurity risk management practices match the characteristics described within the Framework—known as the Framework Implementation Tiers. *Id.* at 32. The Tiers provide a measurement for how organizations view and manage cybersecurity risk, taking into consideration an organization's current practices, the cyber threat environment, legal and regulatory requirements, business objectives, and organizational constraints, among other considerations. *Id.*

While the Framework's Implementation Tiers gauge the degree and sophistication of an organization's overall cybersecurity risk management practices, the Framework Profiles are meant to align the particular Framework Core Functions, Categories, and Subcategories with an organization's own implementation scenarios. *Id.* Overall, the drafters of the NIST Framework expressed that successful implementation of the Framework is based on an organization's ability to achieve its targets. *See id.*

Because no comprehensive cybersecurity standard of care exists, the NIST Framework has the potential to, at the very least, assist in the definition of the national standard of care.

Voluntary Cybersecurity Frameworks in the Global Context

In addition to the NIST Framework, various global frameworks for cybersecurity standards have emerged.

For example, British Standard 7799 was prepared for business managers and their staff to provide a model for setting up and managing effective Security Management Systems. It is a comprehensive set of controls comprising of best practices in information security in the United Kingdom. British Standard 7799 gives recommendations for information security management for use by those responsible for initiating, documenting, implementing or maintaining security in their organization. It also specifies requirements for establishing, implementing, and documenting information security management systems.

Additionally, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) also provide best practice recommendations on information security management and program elements. ISO/IEC 27002:2005. ISO defines the broadest structure of an effective overall program, supporting information security as a systems issue that includes technology, practice, and people, and describes the need for a formal security program.

Given the various available options defining cybersecurity best practices, how can an attorney know how to advise his or her clients as to the current standard of care?

So What is the Standard of Care?

Legal compliance with current United States cybersecurity law relies heavily on interpreting and implementing "reasonable" and "appropriate" cybersecurity measures. Negligence law relies on oftentimes-amorphous standards of care; while statutes like the FTC Act require covered institutions to provide reasonable security safeguards. Given that what constitutes "reasonable" cybersecurity practices is not yet well defined, the NIST Framework has the potential to be influential in shaping reasonable cybersecurity standards in the United States and further afield.

What exactly is "reasonable" is itself open to interpretation. It may mean: (1) reasonable efforts to prevent unauthorized access to, and use of, data processing systems; (2) maintaining a record to verify access and use of data processing systems; (3) reasonable efforts to secure Personal Data against unauthorized destruction or loss; and (4) reasonable efforts to ensure that Personal Data is not kept for longer than necessary. Courts, however, have found that it does not necessarily infer "state of the art" facilities, technologies, or business practices. Because of the ambiguity that can surround reasonableness, reliance on industry standards has been used as a guidepost for assessing reasonable conduct.

Thus, attorneys may advise their clients that company practices and procedures should be rooted in concepts of reasonableness. Adherence to industry practice, in turn, may be viewed as reasonable and provide a defense in some cases in the event of litigation.

Ethical Obligations as an Attorney

In addition to the standard of care, attorneys should also be wary of ethical obligations that arise in the cybersecurity context.

There are three principal ethics rules that address an attorney's protection of cyber data.[3]

First, Rule 1.1 of the Model Rules of Professional Conduct admonishes that "a lawyer shall provide competent representation to a client." The rule defines "competent representation" as requiring "the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation." Model Rule of Prof'l Conduct R. 1.1. And commentary to the rules states that "[t]o 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*." *Id.* at cmt. 8 (emphasis added). As a result attorneys working with sensitive cyber data or using cloud computing technology must have the requisite understanding of how the technology will affect their clients.

Second, Rule 1.6 of the Model Rules of Professional Conduct requires attorneys 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 the commentary to the rule provides, what constitutes a

[3] *See* Matthew Murphy, *Legal Ethics of Cloud Computing*, DRI For the Defense (July 2014).

"reasonable effort" depends upon several factors, including (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 lawyer's ability to represent clients." Model Rules of Prof'l Conduct R. 1.6 cmt. 18.

Finally, although attorneys are permitted to use third-party vendors to analyze or to store client data, attorneys are obliged to make reasonable efforts to ensure those vendors also safeguard client information. *See* Model Rules of Prof'l Conduct R. 5.3 & cmt. 3. What constitutes a "reasonable effort" depends upon the nature of the service involved, the terms of the service, and the legal environment of the jurisdiction in which the service is provided. *Id.*

Because the rules of professional responsibility are adaptable to new technologies, attorneys must inform themselves of the risks of inadvertent or unauthorized disclosure of client's cyber data and take reasonable and information-appropriate measures to reduce those risks.

II. How to Meet the Standard of Care?

Given all of these different (and sometimes conflicting) standards, how can an individual or business keep track and avoid liability?

The piecemeal regulation in this area certainly does not make it easy on individuals or businesses; however, there are some best practices that attorneys and businesses can adopt, depending on the type of data that they use, store, or transfer that can help prevent data breaches or minimize the liability resulting from a data breach. Some of these best practices include:

1. Know your data;
2. Update your technical safeguards;
3. Use secure vendors; and
4. Implement data security policies.

Know Your Data

No matter what kind of sensitive data you may be responsible for, the first step to securing that data is to know what it is and where it is located. The reasonable level of security may be different for different types of data and it is important to know what kind of data you are dealing with in order to maintain the proper safeguards. Part of this process involves mapping the sensitive data under your control and partitioning sensitive data from general-use data.

Update Your Technical Safeguards

Once you know what data is stored where, it is critical to take steps to secure and protect the information. The amount of protection required will ultimately depend on the type of data, but sensitive information, including personal identity information, trade secret information, and proprietary client data, should at least be protected by industry-standard technical security mechanisms. Examples of these include encryption, strong passwords, two-factor authentication, antivirus, firewall, and data loss prevention programs. Depending on the sensitivity of the data, one or more of these technologies may be appropriate. Therefore, it is important to know the type of information that needs to be secured and the expectations for securing that information.

Use Secure Vendors

The best cybersecurity policies and practices in the world are insufficient if your vendors do not have robust cybersecurity practices and policies. It is critical that all third-party vendors who have access to your network or sensitive data maintain sufficient security mechanisms on their end. Vendors can be easy access points for hackers and malware and therefore you will want to ensure they meet minimum-security standards appropriate for the access that they have.

Implement Data Security Policies

One of the best ways to be prepared for a cyber attack is to have policies and plans in place to try to prevent such attacks and to respond appropriately to any such event. At a minimum, these plans should address, the minimum physical, technical and administrative safeguards. They should also include a plan to respond to an actual or threatened breach (as discussed in Section III). Having plans and procedures in place are the best way to ensure that your response to a breach is prompt, orderly and appropriate. A breach response plan also goes a long way to mitigate the chaos that often results from a breach (not to mention the potential to help mitigate liability and damages stemming from the breach).

Additional Responsibilities for Specific Data

In addition to following the above general best practices, it is important to understand that certain types of data require specific procedures and may follow a different standard of care.

Financial Information

Financial institutions are required to "protect the security and confidentiality of those customers' nonpublic personal information."

The FTC's "Safeguard Rule" requires covered financial institutions to "develop, implement, and maintain a comprehensive information security program" that "contains administrative, technical, and physical safeguards that are appropriate to [an organization's] size and complexity, the nature and scope of [an organization's] activities, and the sensitivity of any customer information at issue." Gramm-Leach-Biley Act ("GLBA"). Pub. L. N. 106-102, 113 Stat. 1338 (1999). This program must be reasonably designed to achieve the objectives of the GLBA.

Health Information

The Health Insurance Portability and Accountability Act ("HIPAA") authorized the Department of Health and Human Services to adopt "national standards that protect the confidentiality and integrity of electronic protected health information," or "ePHI." Pub. L. No. 104-191, , §1173, 110 Stat 1938 (1996) (codified as amended at 42 U.S.C. § 1320d et seq.).

Under the HIPAA Security Rule, covered entities must "assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected." *Id.*

Online Information – Digital Assets

"Digital assets" include an individual's smartphone, computer, electronically stored information, online accounts, ability to pay bills online, rights to online accounts, internet domain names, and other digital property. When an individual becomes incapacitated or after an individual dies, there are significant challenges that fiduciaries (or attorneys) may face when dealing with that individual's digital assets.

Studies show that ninety-three percent of Americans who have digital assets were unaware or misinformed about what happens to their digital assets when they die. Harris Poll (March 2013).

To date, at least five states have enacted laws that relate to digital assets with regard to estate planning. The earliest from Rhode Island and Connecticut are limited in scope to email accounts. A 2007 statute from Indiana includes "electronically stored documents of the deceased." A 2010 statue from Oklahoma covers the broader notion of digital assets. In 2011 Idaho passed a bill based upon the Oklahoma one. Currently, Texas has no laws regarding digital assets with regard to estate planning.

Over the last few years the Uniform Law Commission's ("ULC") Fiduciary Access to Digital Assets committee has worked with companies, private organizations, and industry leaders to craft a model act to incorporate digital assets into probate and trust codes. The ULC committee recently prepared a draft of the Uniform Fiduciary Access to Digital Assets, which is intended to "vest fiduciaries with at least the authority to manage and distribute digital assets, copy or delete digital assets, and access digital assets." See FIDUCIARY ACCESS TO DIGITAL ASSETS ACT, REVISED (2015), National Conference of Commissioners of Uniform State Laws, available at http://www.uniformlaws.org/shared/docs/Fiduciary%20Access%20to%20Digital%20Assets/revised%202015/2015_RUFADAA_Final%20Act_2015dec11.pdf.

When there is a death event, the potential for a cyber threat increases. This is even truer with digital assets so it is especially important to advise your clients to plan who controls their passwords and digital assets. Failing to manage digital assets open can leave the decedent vulnerable to identity theft by those who may be able to hack into the decedent's accounts.

The first among many challenges in this regard, is to find the individual's digital property and identify which digital property is valuable or significant. Then, fiduciaries or attorneys have several additional, significant digital property obstacles to overcome, including: (1) passwords; (2) encryption; (3) federal and state criminal laws that penalize "unauthorized access" to computers and data (including the Computer Fraud and Abuse Act); and (4) federal and state data privacy laws (including the Stored Communications Act).

III. Breach & Breach Reporting

Data breaches are all over the news these days. High-profile data breaches are front-page news and people are more concerned than ever about data breaches and identity theft. Many of these stories involve mysterious hackers or sophisticated state-sponsored intrusions and millions of dollars-worth of sensitive information; however, the majority of data breaches are far-less newsworthy, yet equally devastating on the affected individuals.

What Is a Breach?

The Department of Justice defines "breach" as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to information, whether physical or electronic. *United States Department of Justice, Instruction, Incident Response Procedures for Data Breaches* (Aug. 6, 2013). It includes both intrusions (from outside the organization) and misuse (from within the organization). *Id.* This definition covers the front-page news attacks such as sophisticated hacks, corporate espionage, and state-sponsored network attacks, but it also includes the more mundane (but potentially equally harmful) incidents such as lost or stolen laptops, disgruntled employees leaving with flash drives full of documents, and phishing.

How Does a Breach Occur?

Breaches do not just happen to high profile targets, breaches occur in just about every type of company and every type of industry. Data breaches can result from complex and persistent hacks or sophisticated corporate espionage, but data breaches can also result from lost smart phones or laptops, improperly destroyed records, or basic malware from unscrupulous websites.

Further, even the most well prepared individuals and businesses can fall victim to a breach. This is because you are only as strong as your weakest access point—whether that is an employee that is not trained or cautious regarding your data security practices or a vendor with network access that does not have security measures that are up to par.

Essentially, anyone and everyone are potential targets of a data breach. Even industries and individuals that do not rely on sophisticated technology or vast connectivity are vulnerable to cyber attack. In fact, experts like to say that there are two types of businesses: those that know they have been hacked, and those that do not know it yet.

You Are Breached, Now What?

Although you take steps to avoid a data breach, your job does not end there. When a breach does occur, it is critical to promptly and appropriately respond. As a victim of a data breach, you will have certain obligations, which if not carried out properly, can turn you into a defendant in a subsequent lawsuit. Additionally, some of these obligations must be carried out in accordance with strict timelines—some within only a few days of the breach. For attorneys, this is especially important given that you may have fiduciary or ethical duties to your clients that would cause you to be held to a higher standard.

Given that multiple jurisdictions have different requirements complicates breach responses. In the United States there are federal and state laws that involve data breach response. Depending on the information/data involved and the scope of the data breach, you may be required by law to notify individuals who may be impacted by the data breach. This notification obligation is very specific, varies from state to state, and, if done incorrectly, could lead to penalties for the breached company. Notification to affected individuals should be timely, conspicuous, and delivered in a manner that will ensure the individuals receive it. In Canada, there is an obligation to notify Canadian citizens if a breach creates a risk of harm for such individuals. The key consideration should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately accessed, collected, used, or disclosed. Europe has even more strict requirements for data security and breach notification.

To be able to meet these requirements you need to have a plan in place. Depending on the size of your business and scope of the data breach your breach response plan may require coordination among several key internal players, including general counsel, information security personnel, IT personnel, HR personnel. Even if you are the sole party responsible for responding to the breach, you will have to consider all of these roles. In addition, whether you are responding alone or as a team, you may need to

involve law enforcement, forensics experts and outside data security counsel.

Although you should take any breach or threatened breach seriously, the actual scope of the investigation and response will depend on the type and severity of the breach. For example, a breach involving personal data or personal identity information will require a more thorough investigation and response than a breach that does not involve such information or data.

Because of the chaos that can follow a data breach, it is important that your breach response plan identifies the response team and outlines their roles and responsibilities. If you are responding to the breach on your own, then you may be responsible for fulfilling all of these roles. Your plan should be designed to comply with notification and reporting requirements for various jurisdictions and the payment card industry, as applicable to your business.

Your breach response team is responsible for managing security incidents involving the loss or unauthorized access of personal data and personal identity information and other security incidents involving sensitive data or network systems. The response team should keep abreast of relevant threats, vulnerabilities or alerts from actual incidents. The team should have the authority to make decisions related to the incident and to make required notifications.

It is critical to get the breach response right. Untimely or inadequate responses could result in fines, increased regulatory scrutiny, lawsuits, administrative actions, reputational damage, lost revenue, or loss of competitive advantage.

Steps in a Breach Response

A prompt and organized breach response is necessary to avoid legal and regulatory penalties. There are generally five steps to a prompt and organized breach response:

1. Discovery and Reporting
2. Initial Response
3. Investigation
4. Remediation
5. Post-Incident Review

Each of these steps involves a series of important phases and tasks.

1. Discovery & Reporting

The first step to responding to a breach is to identify the incident and report the incident to the proper parties. Personnel who receive or discover information regarding a breach or potential breach should report such information to those responsible for responding to the breach. Upon notice of a breach or potential breach, the responsible party should activate the full response team, if applicable, and implement the breach response plan.

Individuals should report breaches or potential breaches through the proper chains immediately upon discovery, but in no event later than 24 hours after discovery.

The key during this stage is to ensure that breaches are identified and quickly reported so that the proper parties are made aware and so that the responsible parties can respond in a prompt, orderly manner.

2. Initial Response

Once a breach incident is reported to a member of the response team, the team members should begin the response in accordance with the breach response policy. This step is critical because the information obtained and the steps taken immediately after discovery can affect the rest of the investigation and ensuing response.

The keys actions during this stage are to (a) determine the scope of the breach, (b) stop the intrusions from spreading further into computer systems, (c) prevent further damage, (d) maintain any evidence, and (e) determine whether sensitive information is involved and whether this triggers notification requirements. The response team should work together to secure and isolate affected systems to limit further data loss and preserve evidence.

3. Investigation

During the investigation stage, the response team, in conjunction with HR personnel, outside counsel and the forensic experts, should launch a full investigation into the incident and the data involved. This step is critical to determine the scope of the breach, identify affected individuals, identify legal requirements, and prepare proper responses.

The key actions during this stage is to determine (a) how the incident occurred, (b) who is responsible for

the incident, (c) what data/information was involved, (d) who's information was compromised, (e) what requirements/obligations the company will have going forward, and (f) what improvements should be made by company to prevent future incidents.

Depending on the scope of the breach, it may be necessary to engage forensic experts to investigate. Forensic experts can help determine how the breach occurred, what systems are effected, what data was compromised, and whether the breach is ongoing. All of this information is important to determine an effective breach response. In addition, if the breach involves a disgruntled employee, it is important to involve the HR department in the investigation and response.

4. Remediation

The next step is to respond to the incident. The response should be tailored (based on the information obtained during the investigation) to mitigate damages, comply with legal requirements, fix affected systems, remove any discovered vulnerabilities, return Company systems online.

The key during this stage is to ensure that all individual responses are coordinated to (a) remove the threat, (b) avoid further damage/loss, (c) repair affected systems, (d) comply with legal requirements (including, without limitation breach notification requirements), (e) remove system vulnerabilities, (f) bring the repaired systems back online, and (g) respond to third-party inquires or make a public announcement (if such an announcement would be prudent).

Depending on the information/data involved and the scope of the data breach, state law and federal regulations may require you to notify individuals impacted by the data breach. This notification obligation is very specific, and failure to follow specific legal requirements, may lead to lawsuits and regulatory penalties. The response team should work closely with outside counsel to ensure that the breach notification, if required, is done properly. State notification requirements may be delayed at the request of law enforcement; therefore, if the breach is significant, it may be helpful to involve law enforcement early in the response process.

Although states have different specific requirements (and thus several different versions of the notification may be necessary), generally, content in notification to individuals should include:

1. A general description of the incident and information to assist individuals in mitigating potential harm, including a customer service number, steps individuals can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies, and sources of information designed to assist individuals in protecting against identity theft.

2. A reminder to the effected individuals to remain vigilant over the next 12 to 24 months and to report incidents of suspected identity theft.

3. Information for each individual regarding the availability of the Federal Trade Commission's (FTC) online guidance regarding measures to protect against identity theft, and encourage individuals to report any suspected incidents of identity theft to the FTC. Typically this includes providing the FTC's Website address and telephone number for the purposes of obtaining the guidance and reporting suspected incidents of identity theft.

5. Post-Incident Review

The response team's job is not complete after the data security incident has been contained and the company is back online. It is imperative to learn from a data breach to be better prepared to deal with the next one. After responding to an incident, the response team should review notes and evidence to better understand existing vulnerabilities and improve response processes. If forensic experts were involved, talk to those experts and review their final report to better understand the vulnerabilities.

The key during this stage is to use the information obtained from the data security incident to (a) better understand and remove vulnerabilities, (b) improve incident response procedures, (c) improve computing systems and technical defenses, (d) aid in any criminal or civil action against the violators, and (e) prevent or limit reputational harm to Company.

Conclusion

Due to the increase in cyber attacks and misappropriation of data from companies of all sizes

and across all industries, attorneys, both personally and professionally, face increasing responsibilities to understand and implement strong and robust data protection programs. Attorneys should be aware of the relevant and changing data protection standards, understand how to meet such standards and help clients to do the same, and prepare to react effectively when a data breach occurs.

External Security Questionnaire

Law Office: This form is intended for use by law firms that provide services for the companies of _____ If a given question does not apply, pleaseso indicate in the comments section.

Answers will be reviewed by an Information Security Analyst at the _____ who may request further clarification.

Law Firm Name	
Address	
Data Center Address (if different from above)	
Name of person completing this form	
Phone #	
Email Address	
Person Accountable for Information Security (if different from above)	
Date Completed	

Location of data: Check all that apply

☐	Data provided by / owned by _____ will be stored internally at the law office location.
☐	Data provided by / owned by _____ will be stored at a another Data Center.
☐	Data provided by / owned by _____ will be stored at a 3rd party location.

General information about this Questionnaire:

This Questionnaire is being used to assure that the Vendors systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability. This Questionnaire is one component of _____ ongoing due diligence and risk management process. IF REFERENCING PUBLISHED POLICIES PLEASE PROVIDE COPIES FOR THE SECURITY ASSESSMENT.

	Organization of Information Security	Responses
1	Allocation of Information Security Responsibilities. Please identify the person or group responsible for information security within your organization? What are the qualifications of that person or group.	

External Security Questionnaire

2	Confidentiality Agreements. Are all personnel with access to ____client, confidential or proprietary information required to sign confidentiality agreements?	
3	Independent Review of Information Security. Are external audits performed to determine regularly compliance and ensure adherence to security policies? If so, please indicate the type (e.g. Internal / External Audits, SSAE16 SOC 1, 2, 3, other) and frequency of audit. Please provide a summary of results for the most recent audit.	

External Security Questionnaire

	External Parties	Responses
4	Identification of Risks Related to External Parties. Does your organization perform risk assessments or other forms of due diligence on third parties (e.g., contracted datacenters) prior to granting system access? Are subcontractors included in this process?	
5	Addressing Security when Dealing with Customers. How are permitted third party connections to the network or datacenter protected?	

	Human Resources Security	Responses
6	Roles and Responsibilities. Are job descriptions documented and sufficiently specific to determine appropriate access levels for all personnel? Please explain the system used for correlating job descriptions and access levels. Is role based access control (RBAC) used?	
7	Screening. For each class of worker (Employee, Contractor, Consultant) for which classes does your organization perform criminal, reference & identity verification checks.	
8	Terms and Conditions of Employment. Are all employees, contractors and consultants required to sign an acknowledgment that they have received, understand and agree to comply with the security policies? Please provide a copy of a blank acknowledgment.	
9	Information Security Awareness, Education, and Training. Is your organization's security training and awareness program administered internally or by a third party? Please describe how the program is tested, at what intervals, and indicate whether all personnel must participate.	

External Security Questionnaire

10	Disciplinary Process. Please provide your organization's disciplinary procedures for information security violations.	
11	Return of Assets. Are all employees, contractors and third party users required to immediately return all organization owned assets in their possession upon termination of their employment, or when they leave the organization contract or agreement?	
12	Removal of Access Rights. Are access permissions terminated promptly if an employee resigns, is terminated, or changes positions? If yes, please describe the procedure.	

	Physical and Environmental Security	Responses
13	Physical Security Perimeter. How is perimeter access to the facility controlled?	
14	Physical Entry Controls. Are all visitors (non-personnel) name, date and time-logged as guests, preauthorized and escorted at all times by appropriate, security trained personnel?	
15	Securing Offices, Rooms, and Facilities. How is physical access to facilities, offices and rooms controlled?	

	Equipment Security	Responses
16	Security of Equipment Off-premises / Physical Media in Transit. Is equipment or media sent or taken offsite for any reason? If yes, state each reason for which such media may be sent offsite (e.g., repairs, off-site data backup) and describe the precautions taken to protect information contained on such media in transit and at the alternate location.	

External Security Questionnaire

17	Secure Disposal or Re-use of Equipment. Please describe how your organization disposes of or recycles its information processing equipment.	
18	Describe your organization's data wiping process for any electronic data storage media including fixed, removable and external devices.	

	Third Party Service Delivery Management	Responses
19	Service Delivery. How are the provision of services or reports under Service Level Agreements (SLAs) with datacenters, ASPs, hosting providers or other third party service providers audited or monitored for compliance? If audited, please indicate the audit frequency.	

	Protection against Malicious and Mobile Code	Responses
20	Controls against Malicious Code. Please describe the solution used to protect servers and workstations from malicious code such as virus, root kits, Trojans, worms, spy ware, pop-ups, spam, scripts, floods, DoS, malware, etc.	

	Network Security Management	Responses
21	Security of Network Services. Are the security services and / or devices that provide protection from internet threats owned and administered by your organization? If not, please provide details.	

	Media Handling	Responses

External Security Questionnaire

22	Management of Removable Media. Please describe your organization's procedures for usage and management of all types of removable media.	
23	Disposal of Media. Describe your organization's procedures for maintenance and destruction of media including paper documents containing sensitive information.	
24	Information Handling Procedures. Please explain procedures for handling and storage of information to protect it from unauthorized disclosure or misuse.	

	Exchange of information	Responses
25	Electronic Messaging. Does your organization have a secure email system for internal and external use? Please describe procedures followed when sending sensitive data to an external party.	

	User Responsibilities	Responses
26	Unattended User Equipment. Are all personnel required to log off or shut down their workstations when the workday is over? Do all workstations lock after a specified period of inactivity? Specify.	

	Network Access Control	Responses
27	User Authentication for External Connections. What solutions are used to provide remote access to your organization's network? Please provide details.	
28	Are modems permitted within your organization's system network? If yes, please explain how these devices and connections are secured.	

External Security Questionnaire

29	Are wireless network devices permitted within your organization's network? If yes, please explain how these devices and connections are secured.	
30	Describe if and how data segregation occurs during backups?	

	Operating System Access Control	Responses
31	User Identification and Authentication. Does a unique ID and password identify each user?	
32	Does your organization permit sharing User IDs or passwords? If yes, please explain the circumstances and mitigating controls used.	
33	Password Management System. Describe password policy - 1) what is the minimum length in characters? 2) Describe the restrictions on password content. 3) Can passwords be reused? 4) How frequent are passwords forced to change? 5) Are passwords visible when being entered? 6) Are passwords stored in encrypted format?	

	Mobile Computing and Teleworking	Responses
34	Mobile Computing and Communications. What type of mobile computing devices are allowed on your network (e.g. laptops, blackberries, PDAs, etc)? Are these devices required to be corporately owned or do you allow personally owned devices to connect?	
35	Are sensitive data stored on the mobile device required to be encrypted? Are other safeguards deployed to protect stored data from unauthorized access or misuse?	
36	Are all communications to and from such devices (e.g. PDAs, blackberries, etc) encrypted?	

	Cryptographic Controls	

External Security Questionnaire

37	Policy on the Use of Cryptographic Controls. If Protected Heath Information, Personally Identifiable Information, or other sensitive data is transmitted over public networks connected to your organization (e.g., Internet), is the data encrypted? If yes, please provide details (algorithm, key size, etc).	

	Technical Vulnerability Management	Responses
38	Control of Technical Vulnerabilities. Does your organization utilize established, documented procedures for patching against vulnerabilities? Describe.	
39	Are external penetration / vulnerability tests performed on a regular basis? Internal or third party? Please describe testing details, including intervals and a summary of results for the most recent test.	

	Information Security Incident Management	Responses
40	Reporting Security Weaknesses. Does organizational policy require information security event reporting by all personnel?	

	Management of information Security incidents and Improvements	Responses
41	Responsibilities and Procedures. Please provide your organization's procedures and reporting/escalation process for handling security incidents. Are all known security violation events logged, monitored, reviewed, reported, investigated and followed up?	
42	Learning from Information Security incidents. Please explain how information gained from the evaluation of information security incidents is used to enhance or implement additional controls in order to limit frequency, damage or cost of future occurrences.	

External Security Questionnaire

	Compliance	Responses
43	Identification of Applicable Legislation. Does your organization regularly update its compliance plan to include all relevant statutory, regulatory and contractual requirements?	
44	Protection of Organizational Records / Data Protection and Privacy of Personal Information. Describe your organization's procedures for safeguarding and preservation records containing Protected Health Information, Personally Identifiable Information or other information subject to data protection and privacy laws (e.g., HIPAA, GLBA, COPPA) and contracts.	
45	Prevention of Misuse of Information Processing Facilities. Identify any bonding/insurance in force that protects clients from financial loss due to employee/ contractor fraudulent acts. Please provide your organization's aggregate and per incident liability limits.	
46	Regulation of Cryptographic Controls. Please provide your organization's procedural controls designed to comply with relevant laws, regulations and agreements regarding the importation, export or use of cryptographic controls such as encryption algorithms.	

	Compliance with Security Policies & Standards, & Technical Compliance	Responses
47	Technical Compliance Checking. Has your organization received any certifications or accreditations from a third party? If yes, please provide a copy of the certification or accreditation documents.	

Ethical obligations and best practices to be used by bankruptcy professionals to protect client confidences and valuable estate property in the era of the data breach

Monsita Lecaroz Arribas
Assistant U.S. Trustee[1]
U.S. Department of Justice
San Juan, PR

[1] The views expressed herein are the views of the author/speaker and are not intended to represent the views of the Department of Justice, the Executive Office for United States Trustees, or any other United States Trustee.

Ethical obligations and best practices to be used by bankruptcy professionals to protect client confidences and valuable estate property in the era of the data breach

I. Introduction

These materials will cover the common terms and definitions, applicable rules and ethical obligations, and desired best practices of professionals to secure client information in their possession to forestall the unwanted disclosure of such information due to a data breach.

II. Common Terms and Definitions

PII is defined as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

To *distinguish* an individual is to identify an individual. Some examples of information that could identify an individual include, but are not limited to, name, passport number, social security number, or biometric data. In contrast, a list containing only credit scores without any additional information concerning the individuals to whom they relate does not provide sufficient information to distinguish a specific individual.

To *trace* an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status. For example, an audit log containing records of user actions could be used to trace an individual's activities.

Linked information is information about or related to an individual that is logically associated with other information about the individual. In contrast, *linkable* information is information about or related to an individual for which there is a possibility of logical association

with other information about the individual. For example, if two databases contain different PII elements, then someone with access to both databases may be able to link the information from the two databases and identify individuals, as well as access additional information about or relating to the individuals. If the secondary information source is present on the same system or a closely-related system and does not have security controls that effectively segregate the information sources, then the data is considered linked. If the secondary information source is maintained more remotely, such as in an unrelated system within the organization, available in public records, or otherwise readily obtainable (e.g., internet search engine), then the data is considered linkable.

This is a list of examples of PII:

- Name, such as full name, maiden name, mother's maiden name, or alias

- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number

- Time and Attendance records

- Leave records

- Telework agreements

- Address information, such as street address or email address

- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people

- Telephone numbers, including mobile, business, and personal numbers

- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)

- Information identifying personally owned property, such as vehicle registration number or title number and related information

- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

The term "breach" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to information, whether physical or electronic. It includes both intrusions (from outside the organization) and misuse (from within the organization).

"Malware" is an umbrella term that can include viruses, worms, Trojans, ransomware, spyware, adware, scareware, wiper software and other malicious, hostile or intrusive software. It can be used to spy or designed to cause harm, destroying or sabotaging systems or data. The recommendations in this paper are concerned with malware that destroys the confidentiality, integrity and availability of data.

III. Government policies

On September 1, 2015 the U.S. Department of Defense and the U.S. Office of Personnel Management announced the award of a $133,263,550 contract to Identity Theft Guard Solutions LLC, doing business as ID Experts, for identity theft protection services for 21.5 million

individuals whose personal information was stolen following one of the largest cybercrimes ever carried out against the United States Government.

Given the recent breach incidents across the government making clear the threat to which we are all exposed, various government agencies have issued warnings and recommendations to that effect, which can be to the benefit of the general public.

The Federal Trade Commission recently published guidance on email hacking which can be found at http://www.onguardonline.gov/articles/0376-hacked-email.[2]

On November 16, 2015 an inter-agency task force (Department of Homeland Security, DHS, Financial Services – Information Sharing and Analysis Center, National Security Agency, National Cyber Security Center of Excellence, and the Security Industries and Financial Markets Association) issued a Notice of Best Practices for U.S. Financial Institutions to reduce the risks associated with destructive malware. Their recommendations are centered on 5 core elements:

Identify - Critical data, backup processes and systems in the organization that are necessary for critical business functions, where it comes from, where located, and where used. Identifying solution components training, vectors, detection technology, ongoing risk assessments and monitoring, information sharing and incident response keeps the enterprise in a continuous state of alert and well positioned to take action promptly.

Protect - A variety of controls are necessary for a comprehensive and robust security framework to protect corporate data and personally identifiable information.

Detect - Speed is essential in detecting malware when it enters a key environment and in preserving the security of the financial sector.

[2] Neither the Department of Justice nor the U.S. Trustee Program controls or guarantees the accuracy, relevance, timeliness, or completeness of any external sites or information, and the agency expressly reserves sole discretion to establish or remove external links from the server at any time. Further, the inclusion of links to particular external sites is not intended to reflect their importance or to endorse any views expressed, products or services offered on those sites, or the organizations sponsoring the sites.

Respond - In the event of unauthorized access, the financial institution's computer systems could potentially fail, and confidential information could be compromised. Management must decide how to properly protect information systems and confidential data while also maintaining business continuity.

Recover - Speed is essential in detecting malware when it enters a key environment and in preserving the security of the financial sector.

Soon thereafter, on November 18, 2015, the FBI issued Public Service Alert 1-42115 with regard to the increased risk of Law Enforcement personnel, Public Officials and their family members, of being targeted by "Hacktivists". The FBI's Internet Crime Complaint Center (IC3) has received complaints regarding hacking collectives leveraging open source, publically available information to target law enforcement officers, their employers, and their family members for cyberattacks, and recommends that law enforcement personnel and public officials maintain an enhanced awareness of the content they post and how it may reflect on themselves, their family, their employer or how it could be used against them in court or during online attacks.

Safeguarding personally identifiable information in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public.

OMB memorandum Safeguarding Against and Responding to the Breach of Protecting Personally Identifiable Information (May 22, 2007).

IV. United States Trustee' policies for trustees

Email accounts for Chapter 7 trustees are not exempt from hacking. In one incident, the hacker proceeded to find an e-mail which the trustee had sent to a depository bank and to which the bank had responded. The hacker then posed as the trustee with a reply e-mail requesting that the bank issue a wire transfer of funds from the trustee's largest asset case. The bank responded and stated that in addition to e-mailed instructions, it would need to verify the transfer with a callback. The hacker, again posing as the trustee, stated that she was out of town attending the funeral of a close relative and would not be able to access a phone until after the time the transfer would be needed. The bank then became suspicious and called the trustee's office, confirming that the transfer request was fraudulent. The hacker apparently blocked the trustee from receiving e-mails which the hacker initiated with the bank. As a consequence, the trustee was not aware of the fraudulent transfer request until the bank provided the e-mail chain to the trustee. In the second incident, the bank received a wire transfer request from the trustee's email account. The request was made on the bank's form, had the correct bankruptcy estate name and bank account number, and the trustee's signature (an obvious cut and paste job). The bank grew suspicious because of the email language and contacted the trustee to confirm if the request was legitimate. The investigation determined that the trustee's Gmail account was hacked by unknown persons.

The above incidents may not be isolated. Trustees must take appropriate security measures to protect estate account funds and information, including the following:

- Change the passwords for current email accounts and use strong alphanumeric passwords.

- Contact their Internet provider, IT advisor or computer software vendor for suggestions they may have.
- Use commercially available software to regularly remove sensitive materials from all devices used to read emails and attachments.
- Do not use a personal email account for trustee business.
- Consider a dedicated email address for communications with banks.
- Contact their depository to review its procedures to verify the authenticity of all communications requesting the transfer of funds from estate accounts and suggest using a callback procedure if it is not currently in place.

The United States Trustee's Handbook for Chapter 7 Trustees (pages 5-15 to 5-21) provides for specific requirements that trustees must comply with, such as:

- imposes specific restrictions on using wire transfers

- requires specific computer security measures

- requires that trustees develop and maintain a business interruption plan

- requires specific records security and retention policies, including individual case records and tax returns.

The Handbook also requires that trustees have rules of behavior governing computer use within their offices, and also provides sample rules of behavior governing computer use for their benefit.

The Chapter 7 Case Administration Manual at section 2-2.11, p. 43-44, as well as the Chapter 7 Trustee Handbook, at pages 5-21, 22, specifically provides that a bankruptcy trustee, immediately upon discovery, report any loss or potential loss of PII to the United States Trustee.

DUTY TO REPORT LOSS OR POTENTIAL LOSS OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

(1) The trustee has a duty to report to the United States Trustee the loss or potential loss of personally identifiable information (PII), including the theft or the accidental loss of bankruptcy papers (such as meeting of creditors notices and final reports), desktop computers, laptops, PDAs, and removable drives such as USB flash drives and CDs. The trustee must report any loss or potential loss upon discovery even though the trustee may have limited information about the loss at that time.

(a) For purposes of this Handbook, the Program has adopted the definition of PII used by the Office of Management and Budget (OMB). OMB defines PII as information which can be used to distinguish or trace an individual's identity, such as name, Social Security number, or biometric records, etc., alone or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth or mother's maiden name, etc.

(b) Information that is not generally considered PII because it is shared by many people includes: first or last name, if common (like Smith or Jones); country, state or city of residence; age (especially if not specific); gender or race; name of school a person attends or workplace; and grades, salary, or job position. However, since this information could be used to identify a person when multiple pieces of it are brought together, even non-PII data such as this should be protected from loss.

(2) Notice to the United States Trustee may be by phone or email and must include a summary of the known details of the breach and any actions taken or proposed to be taken in response.

(3) Once the trustee has identified the scope of the loss or potential loss, the trustee must determine the appropriate course of action, the level of notification to affected individuals, the resources needed, and any appropriate remedial actions. 28 U.S.C. § 586. Some of the risk factors that the trustee may use to determine the appropriate response are: sensitivity of the data lost, amount of data lost and number of individuals affected, likelihood data is usable or may cause harm, likelihood the data was intentionally targeted, strength and effectiveness of security technologies protecting data, nature of the data (operational or personal), and ability of the trustee to mitigate the risk of harm.

(a) Notification to Third Parties: The trustee must notify law enforcement authorities, the trustee's computer service provider, and insurance carriers, as appropriate. 28 U.S.C. § 586.

(b) Notification to Affected Individuals: The determination of the appropriate level of notification should take into consideration the risk the data loss poses to the individuals. At a minimum, the trustee must notify the affected individuals if the loss involves full social security numbers, or banking, credit card or other financial PII. The trustee must also review state law to determine if there are any state law requirements that govern notifications to affected individuals. Examples of non-state specific notification letters can be obtained from the United States Trustee. 28 U.S.C. § 586.

Compliance with appropriate security measures to protect estate records and PII is not simply recommended by the United States Trustee but is monitored through audits, field exams, and communications with trustees.

V. Applicable Rules

Adding to the existing and undeniable hacking threat, there are several Rules which require attorneys to secure their clients' information in this era of flourishing technology, which encompass national, local rules and ethics rules. These rules cover filings with the Court's electronic filing system, maintenance and security of electronic and paper files, as well as all other attorney-client communication.

a. U.S. Courts Rules

On a national level, the Office of Administrative Courts issued a United States Courts Privacy Policy for Electronic Case Files which is the basis for Rule 5.2 of the Federal Rules of Civil Procedure, Privacy Protection For Filings Made with the Court, adopted in compliance with section 205(c)(3) of the E-Government Act of 2002, Public Law 107–347. Section 205(c)(3) requires the Supreme Court to prescribe rules "to protect privacy and security concerns

relating to electronic filing of documents and the public availability . . . of documents filed electronically." It is meant to address the security and privacy concerns raised by electronic filing. Rule 5.2 provides that unless the court orders otherwise, in an electronic or paper filing with the court which includes "personal data identifiers" the party or nonparty making the filing may include only:

(1) the last four digits of the social-security number and taxpayer-identification number;

(2) the year of the individual's birth;

(3) the minor's initials; and

(4) the last four digits of the financial-account number.

The redaction requirement does not apply to the following:

(1) a financial-account number that identifies the property allegedly subject to forfeiture in a forfeiture proceeding;

(2) the record of an administrative or agency proceeding;

(3) the official record of a state-court proceeding;

(4) the record of a court or tribunal, if that record was not subject to the redaction requirement when originally filed;

(5) a filing covered by Rule 5.2(c) or (d); and

(6) a pro se filing in an action brought under 28 U.S.C. §§2241, 2254, or 2255.

On a local level, the Puerto Rico U.S. District Court issued Advisory 08-08 Regarding Proper Redaction of Information. Rule 5.2 of the Local Rules for the District of Puerto Rico provides for privacy protection for filings made with the Court, in compliance with the policy of the Judicial Conference of the United States and the EGovernment Act of 2002 above stated.

Moreover, through Local Bankruptcy Rule 9037-1, our local Bankruptcy rules squarely impose the responsibility for redacting on the filing parties.

Rule 9037-1
Privacy Protection
(a) Responsibility for Redaction of Personal Identifiers. The responsibility for redacting the personal identifiers enumerated in Fed. R. Bank. P. 9037(a) rests solely with counsel and the parties.
(b) *Sua Sponte* Protective Orders. The court may enter a *sua sponte* protective order where a document has been filed that includes unredacted information prohibited by Fed. R. Bank. P. 9037(a) or information protected under 11 U.S.C. § 107.
(c) Compliance with Electronic Transcripts Policy. Access to every electronic transcript filed with the court will be available at the clerk's office for inspection only, for a period of ninety (90) days after it is delivered to the court to allow interested parties the opportunity to review the transcript and file a Notice of Redaction requesting that personal data identifiers be redacted prior to the transcript being made available to the public. During the ninety (90) day period, a copy of the transcript may be obtained from the transcriber upon payment of the applicable fee. Attorneys who obtain transcripts from the transcriptionist may obtain remote electronic access to the transcript through the court's CM/ECF system for the purpose of creating hyperlinks to the transcript in court filing and for other purposes. After the ninety (90) day period has ended, the filed transcript will be available for inspection and copying in the clerk's office and from CM/ECF through PACER. It is the responsibility of the parties to monitor the docket for the filing of the transcript.
(1) Procedure for Filing a Notice of Redaction. Each party wishing to redact from a transcript personal data identifiers described in Fed. R. Bank. P. 9037(a) must, within seven (7) calendar days of the filing of the electronic transcript, file with the clerk and serve the transcriber with a Notice of Redaction of personal data identifiers.
(2) Statement Required. Within twenty-one (21) calendar days from the filing of the transcript, the party who filed a Notice of Redaction must file with the court and serve the transcriber with a statement indicating the page and paragraph numbers of the transcript where the personal data identifiers are located.
(3) Motion for Additional Redactions to the Transcript. During the twenty-one (21) days period, an attorney may file a Motion for Additional Redactions to the transcript. The transcript shall not be electronically disseminated until the court has ruled upon any such motion.
(4) Once a transcript is redacted, access to the unredacted version of the transcript shall be permanently restricted to viewing at a public terminal in the clerk's office.
(d) Digital Audio Files of Court Proceedings. If information subject to the judiciary's privacy policy is stated on the record, it will be available in the audio files over the internet. Parties must comply with (a) above and avoid introducing personal data and other sensitive information into the record, unless necessary to prove an element of the case. Clerk's office staff cannot redact audio files before they are placed on CM/ECF. If private information is mentioned during a hearing or trial, the parties may move the court to seal, restrict, or otherwise prohibit placement of the digital audio file of the hearing or trial on the internet through the PACER system.

Parties must remember that any personal information not otherwise protected by sealing or redaction will be made available over the internet. Counsel should notify clients of this fact so that an informed decision may be made on what information is to be included in a document filed with the court.

The clerk is not required to review documents filed with the court for compliance with these rules. The responsibility to redact filings rests with counsel and the party or nonparty making the filing.

b. ABA Model Rules of Professional Conduct

The Model Rules of Professional Conduct of the American Bar Association apply to Puerto Rico attorneys in bankruptcy practice pursuant Local Rule 83(k)(b) of the U.S. District Court for the District of Puerto Rico, made applicable through Local Rule 1001 of the Bankruptcy Court for the District of Puerto Rico.

The Model Rules of Professional Conduct also cover the confidentiality of client information.

Rule 1.6: Confidentiality of Information
Client-Lawyer Relationship

(a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).
(b) A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:
(1) to prevent reasonably certain death or substantial bodily harm;
(2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;
(3) to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;

(4) to secure legal advice about the lawyer's compliance with these Rules;
(5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;
(6) to comply with other law or a court order; or
(7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client.
(c) 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.

It is interesting to what extent the U.S. District Court in Puerto Rico, citing said Model Rules, has enlarged the scope of the duty of confidentiality.

> **The duty of confidentiality is far broader than the narrow duty underpinning the attorney-client privilege. See Model Rules of Professional Conduct Rule 1.6, n.3 (2003). As one of the hallmarks of the attorney-client relationship, confidentiality is of grave importance.** It is incontrovertible that even where the privilege does not apply, a lawyer owes a duty of care in protecting the confidences of a client, even those of a prospective client with whom no attorney-client relationship is formed. See ABA Comm. on Ethics and Professional Responsibility, Formal Op. No. 90-358, Sept. 13, 1990.
>
> ***United States v. Morrell-Corrada***, 343 F Supp 2nd 80, 88 (2004).

c. Puerto Rico Code of Professional Ethics

Although not as specific as the Model Rules of Professional Conduct, the Puerto Rico Code of Professional Ethics also imposes the same responsibility on attorneys in this jurisdiction.

Canon 21. Conflicting interests

The lawyer has the obligation to represent his client with complete loyalty. This duty includes the obligation to disclose to the client all the circumstances of his relations to the parties and to third persons, and any interest in the controversy which might influence the client in the selection of counsel. No lawyer should accept employment when his professional judgment might be affected by his personal interests.

It is unprofessional to represent conflicting interests. Within the meaning of this canon, a lawyer represents conflicting interests when, in behalf of one client, it is his duty to contend for that which duty to another client requires him to oppose.

The obligation to represent the client with fidelity includes not divulging his secrets or confidences and to adopt adequate measures to avoid disclosure thereof. A lawyer should not accept the representation of a client in matters adversely affecting any interest of a former client, nor should he be an arbitrator, especially when the former client has made him confidences which may affect one or the other client, even though both clients consent thereto. It will be highly improper for a lawyer to use the confidences of a client to the latter's prejudice.

A lawyer who represents a corporation or partnership owes complete loyalty to the corporation and not to its partners, directors, employees or shareholders, and he may only represent the interests of said persons when the same are not in conflict with those of the corporation or partnership.

When a lawyer represents a client by recommendation of another person or group who pays the lawyer for said service, he should withdraw from the representation of both as soon as a situation of conflicting interests arises between the person or group who pays his fees and the person whom he represents.

An attorney has duty of complete loyalty to his client. Therefore, he cannot represent his client while holding interests in conflict with those of his client. The cannon defines as "conflicting interests" when, for the benefit of a client, the attorney would need to act in such a way that would harm the interests of another client. Another derivative of that duty is the obligation not to disclose any secrets or confidences of the client, and to take appropriate measures to prevent their disclosure. Obviously, the attorney cannot use the client's confidences for his own benefit or to prejudice his client.

VI. Best Practices

With the changing landscapes of law and technology, what can a law firm do to protect confidential client information in the digital age? At a minimum, firms should create and implement information, social networking and document management policies according to the needs of each client.

The attached article, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data,* was written by Drew T. Simshaw and was published in the American Journal of Trial Advocacy, Vol. 38, 2015. We are grateful to Mr. Simshaw and to the American Journal of Trial Advocacy for granting us permission to include this article in our materials.

Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data

Drew T. Simshaw[†]

Abstract

New technologies are drastically changing the way lawyers practice law. Advances in areas such as cloud computing and mobile devices are enabling new ways to communicate with clients, as well as new ways to collect, store, and manage data pertaining to their cases. This Article provides practitioners with the necessary tools to fulfill their ethical obligation to protect client information in an increasingly digitized world.

Introduction

The message of an August 2014 American Bar Association (ABA) resolution was loud and clear: "The threat of cyber attacks against law firms is growing."[1] Like many other professions, "the widespread use of electronic records and mobile devices" by lawyers and law offices present "unprecedented challenges."[2] As *The ABA Cybersecurity Handbook*[3] explains, "Creating, using, communicating, and storing informa

---

[†] B.A. (2007), University of Washington; J.D. (2012), Indiana University Maurer School of Law. Drew Simshaw is a teaching fellow at the Georgetown University Law Center in the communications and technology clinic of the Institute for Public Representation. He previously served at Indiana University with the Center for Applied Cybersecurity Research (CACR) and the Center for Law, Ethics, and Applied Research in Health Information (CLEAR). He is a proud AmeriCorps alum. In law school, he was articles editor for the *Federal Communications Law Journal* and served as postdoctoral fellow in information security law and policy. The author's views in this article are his own, and do not represent legal advice. He thanks Andrew A. Proia, Craig Jackson, and members of the Indiana State Bar Association Legal Ethics Committee for their input on this Article.

[1] American Bar Association, *Cybersecurity Legal Task Force Section of Science & Technology Law, Report to the House of Delegates: Resolution 109* (August 2014) at 4 [hereinafter ABA Cybersecurity Resolution], *available at* http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2014_hod_annual_meeting_109.authcheckdam.pdf.

[2] *Id.*

[3] JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS (2013) [hereinafter ABA CYBERSECURITY HANDBOOK]. The book describes itself as "a

tion in electronic form greatly increases the potential for unauthorized access, use, disclosure, and alteration, as well as the risk of loss or destruction."[4] Lawyers must understand these risks in order to protect confidential client information while practicing law in the age of hackers.

Law firms are especially attractive targets to hackers. This attractiveness is largely because of two compounding perceptions about law firms: that they are valuable targets and that they are easy targets.[5]

First, consider how valuable law firms appear to hackers, particularly for the amount of information they collect, manage, and store. The ABA Cybersecurity Resolution notes that lawyers and law offices "collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery,"[6] not to mention transaction information and financial records pertaining to their clients and themselves. To hackers, a law firm represents the opportunity for a hack that is more efficient than going after a firm's individual clients—after all, "lawyers are usually involved in only their client's most important business matters, meaning hackers may not need to sift through extraneous data to find the more valuable information."[7]

This first reason for attractiveness to hackers is unavoidable; law firms by their very nature will always have many clients and will always hold vast amounts of valuable information pertaining to their cases.

But law firms are also targeted because they are viewed as easy targets—"perceived to have fewer security resources than their clients,

---

powerful and effective tool that attorneys, law firms, in-house counsel and business professionals should utilize in understanding, planning for and responding to a cyber breach." *Id.* at xi.

[4] *Id.* at 41.

[5] *See* JANE LECLAIR & GREGORY KEELEY, CYBERSECURITY IN OUR DIGITAL LIVES, 128 (2015); *see also* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 3, 37 (describing law firms as "soft" and "attractive" targets and also describing lawyers and law firms as "high-priority" targets for cyber-attacks).

[6] ABA Cybersecurity Resolution, *supra* note 1, at 4.

[7] LECLAIR & KEELEY, *supra* note 5, at 128; *see also* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 127 ("[A]ttacks on law firm computers are likely to provide the hacker with more sensitive information per breach of a computer server or hard drive than an attack on the firm's client.").

with less understanding of and appreciation for cyber risk."[8] There is no shortage of clever analogies that demonstrate this dangerous (even embarrassing) vulnerability of law firms. Law firms have been described as the backdoors[9] or gates[10] into their clients, and as "the soft underbelly of corporate cybersecurity."[11] But perhaps most frequently, and most appropriately, law firms have been called out as the "weak link" in a client's data security efforts.[12] In 2013, then ABA President Laurel G. Bellows aptly warned lawyers that "[w]e're fooling ourselves if we think there aren't efforts to reach client information through us."[13]

---

[8] LECLAIR & KEELEY, *supra* note 5, at 128; *see also* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 105 ("Law firms are viewed as a 'very target-rich environment' with significantly less cybersecurity protection in place than their clients have.") (citing John Reed, *The New Cyber Vulnerability: Your Law Firm*, FOREIGN POLICY (Nov. 7, 2012, 8:35 PM), http://foreignpolicy.com/2012/11/07/the-new-cyber-vulnerability-your-law-firm).

[9] *See, e.g.*, David G. Ries, *Cyber Security for Attorneys: Understanding the Ethical Obligations*, LAW PRACTICE TODAY, at 1 (Mar. 2012), http://www.americanbar.org/content/dam/aba/publications/law_practice_today/cyber-security-for-attorneys-understanding-the-ethical-obligations.authcheckdam.pdf ("[H]ackers see attorneys as a back door to the valuable data of their corporate clients."); Ralph Losey, *The Importance of Cybersecurity to the Legal Profession and Outsourcing as a Best Practice—Part One*, E-DISCOVERY TEAM, http://e-discoveryteam.com/2014/05/11/the-importance-of-cybersecurity-to-the-legal-profession-and-outsourcing-as-a-best-practice-part-one ("[B]ad hackers, known as crackers, have learned that when they cannot get at a company's data directly, usually because it is too well defended, or too risky to attack, there is often a back door to this data by way of the company lawyers.").

[10] *See, e.g.*, James Podgers, *Threat of Cyberattacks Must Be Recognized and Responded to, ABA President Urges Lawyers*, ABA J. (Feb. 1, 2013, 7:50 AM), http://www.abajournal.com/mobile/mag_article/aba_president_laurel_bellows_urges_lawyers_to_recognize_respond_to_the_thre (quoting past ABA President Laurel G. Bellows's point that law firms "serve as 'gates' into their clients").

[11] *See* Losey, *supra* note 9.

[12] *See, e.g.*, Matthew Goldstein, *Law Firms Are Pressed on Security for Data*, N.Y. TIMES (Mar. 26, 2014), http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/?_r=0 (describing how FBI officials and security experts have warned that "law firms remain a weak link when it comes to online security"); Daniel Garrie, *Attacking the Weakest Link: BYOD in the Law Firm Culture*, HUFFINGTON POST (Sept. 10, 2013, 5:40 PM) http://www.huffingtonpost.com/daniel-garrie/attacking-the-weakest-lin_b_3862354.html ("The simple principle of attacking the weakest link often may lead back to law firms' devices, as they often do not invest in the technology, people, and cultural awareness necessary to provide strong security.").

[13] Podgers, *supra* note 10 (quoting Laurel G. Bellows).

This second reason for attractiveness to hackers, the legal profession can do something about. Law firms will always be valuable targets, but they do not always have to be easy ones.

Understanding, appreciating, and confronting the data security challenges in today's legal world requires an appreciation for the unique nature of the profession, including its obligations and responsibilities—all of which are accounted for in the profession's rules of professional conduct. These rules provide a valuable lens through which to view the data security challenges of practicing law in the age of hackers and the critical roles that members of the profession play in protecting client data. In order to understand these obligations and how to meet them, lawyers must first understand the nature of the threats, the consequences, and how the lawyers' practice is affected.

I. The Threats, the Actors, and the Stakes

It is clear why firms are attractive to hackers. To truly appreciate the threats facing law firms, however, lawyers must understand not only why their profession is being targeted, but also by whom and with what motives and methods—all of which vary greatly. "Malicious insiders" may hope to embarrass a firm or advance their own pecuniary interest.[14] "Social engineers" are becoming increasingly common and effective at utilizing techniques such as "targeted phishing attacks" that compromise a firm's network by installing malicious software and backdoors.[15] Motivated by everything from economic espionage to advancement of political interests, State-sponsored attackers are becoming increasingly sophisticated,[16] striking even well secured systems with "advanced persistent threats" and "distributed denial of service" attacks.[17] According

[14] LECLAIR & KEELEY, *supra* note 5, at 128; *see also* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 20-21.

[15] LECLAIR & KEELEY, *supra* note 5, at 128-29. In 2014, representatives from several large law firms privately told the *New York Times* that "email 'phishing' schemes seeking to access personal information or account passwords" were the most common "hacker attacks" against the firms. Goldstein, *supra* note 12.

[16] *See* Goldstein, *supra* note 12 ("The main concern for the F.B.I. was state-sponsored hackers breaching a law firm computer system to tap into information about what American corporations were doing.").

[17] LECLAIR & KEELEY, *supra* note 5, at 129.

to IBM's 2013 Security Services Cyber Security Intelligence Index, roughly half all of attacks can be categorized as "opportunistic," and nearly a quarter relate to industrial espionage, financial crime, terrorism, or data theft.[18] Other motivations include an insider's dissatisfaction with their employer or job, social activism, and civil disobedience.[19] Of course, many of the motives for attacking law firms have to do with money.[20] Firms may even need to worry about threats from other firms.[21]

The threats posed by these actors are not going unrecognized. Data security was ranked as one of the top concerns of both directors and general counsel in a 2014 survey of 500 such representatives, and "IT/cyber risk was chosen by . . . 33% of general counsel as an issue they will spend significant time on."[22]

Large organizational clients are also rightly taking notice.[23] Corporate clients are making demands that are "forcing the law firms to clean up their acts."[24] For example, in 2014, the New York Times reported that "Wall Street banks are pressing outside law firms to demonstrate that their computer systems are employing top-tier technologies to detect and

---

[18] *The 2013 IBM Cyber Security Intelligence Index*, IBM.COM (2013) [hereinafter *IBM Cyber Security Intelligence Index*], *available at* http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html. This threat landscape could be changing in the coming years. *See* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 126 (describing how "attacks are evolving from merely opportunistic to sophisticated, targeted attacks in the form of advanced persistent threats (APTs) originating from nation-state actors").

[19] *IBM Cyber Security Intelligence Index*, *supra* note 18.

[20] *See* Garrie, *supra* note 12 ("Like most enterprises, hacking is generally about making money.").

[21] *See* Tom Harper, *The Other Hacking Scandal: Suppressed Report Reveals That Law Firms, Telecoms Giants and Insurance Companies Routinely Hire Criminals to Steal Rivals' Information*, THE INDEPENDENT (June 22, 2013), http://www.independent.co.uk/news/uk/crime/the-other-hacking-scandal-suppressed-report-reveals-that-law-firms-telecoms-giants-and-insurance-companies-routinely-hire-criminals-to-steal-rivals-information-8669148.html.

[22] FTI Consulting and NYSE Governance Services, *Law in the Boardroom in 2014*, FTI CONSULTING (May 19, 2014), http://www.fticonsulting.com/global2/critical-thinking/reports/law-in-the-boardroom-in-2014.aspx.

[23] *See* Garrie, *supra* note 12 (describing why "the increasing number of hacks should leave clients questioning the strength and security with which their law firm protects their data").

[24] *See* Goldstein, *supra* note 12.

deter attacks from hackers bent on getting their hands on corporate secrets either for their own use or sale to others."[25]

As a whole, the legal profession is beginning to take notice of these threats, but lawyers need to be more proactive in confronting them, especially considering the serious consequences that can result from a cyber-attack affecting clients, law firms, and individual members of the profession.

In addition to the possibility of destroying the attorney-client privilege, "[c]lients and third parties may find themselves victims of fraud, identity theft, and bankruptcy, not to mention negative publicity and tarnished business reputation."[26] Under certain circumstances, affected clients and third parties could also face civil actions, administrative proceedings, or even criminal charges.[27] Law firms that fail to employ reasonable cybersecurity measures can face discipline from courts, government investigations, fines, private law suits, and malpractice claims by clients, in addition to irreparable harm to the reputation of the firm and its members due to lost trust of clients, judges, the legal community, and the public.[28]

The ABA Cybersecurity Handbook stresses to lawyers that "information security is not just good business practice; it is becoming a legal obligation."[29] Like many other professions, "[a]ttorneys . . . have common law duties to protect client information and may have contractual and regulatory duties."[30] Lawyers also have special duties that are unique to the legal profession, subjecting them to potential discipline from state ethics boards if they violate their rules of professional conduct.[31] If properly utilized by the legal profession as a whole,

---

[25] *Id.*

[26] LECLAIR & KEELEY, *supra* note 5, at 129.

[27] *Id.*

[28] *Id.*

[29] ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 45.

[30] Ries, *supra* note 9, at 1; *see also* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 41-45 (describing the various sources of a lawyer's duty to provide data security, including statutes and regulations, common law obligations, rules of evidence, rules of professional responsibility, contractual obligations, and self-imposed obligations).

[31] *See* Ries, *supra* note 9 (describing "the rising number of law firm computer intrusions," and that "[a]ttorneys' ethical obligations include understanding and dealing with these threats").

attention to and promotion and enforcement of legal ethics rules could have a profoundly positive effect on proactively improving data security in the practice of law.

II. The Rules

Understanding the role of legal ethics in the age of hackers requires an understanding of several sources that establish and provide guidance on the ethical obligations of lawyers. First, lawyers must be familiar with the ethics rules. Every state has its own rules of professional responsibility, but most are based on the ABA's Model Rules of Professional Conduct.[32] Although states adopt amended versions of the model rules at different paces, all lawyers should be aware of the amendments made to the ABA Model Rules in 2012, which were based on the recommendations of the ABA Commission on Ethics 20/20.[33] Lawyers must also be mindful of opinions by state ethics boards, which provide additional guidance on ethics and data security. There are also a host of secondary sources for guidance, notably *The ABA Cybersecurity Handbook*.[34]

A. Competence

Competent representation of clients is central to all lawyers' ethical obligations. Under the ethics rules of most states, "[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation

---

[32] *See generally* ABA MODEL RULES OF PROF'L CONDUCT, *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html.

[33] *See generally ABA Commission on Ethics 20/20*, AMERICAN BAR ASS'N (Feb. 11, 2013) http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html ("The ABA Commission on Ethics 20/20 was formed to consider changes to the Model Rules of Professional Conduct with an eye in part on the intersection of lawyers' conduct and advances in technology."); John M. Barkett, *More on the Ethics of E-Discovery: Predictive Coding and Other Forms of Computer-Assisted Review*, 2 (2014), *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2015-winter-leadership/010515_ethics_2015__don_t_get_tangled_in_the_web.authcheckdam.pdf.

[34] *See generally* ABA CYBERSECURITY HANDBOOK, *supra* note 3.

reasonably necessary for the representation."[35] While knowledge of data security may be necessary for proper "thoroughness and preparation" in some cases, such knowledge is becoming an increasingly central component of necessary everyday "legal knowledge" and "skill" for lawyers. In most states, comments to this rule explain that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice."[36] When reviewing the Model Rules in light of new technology in 2012, an ABA resolution acknowledged that the duty to "keep abreast of changes in the law and its practice" implicitly encompasses understanding relevant technology's benefits and risks.[37] Nevertheless, the resolution also expressed that "it is important to make this duty explicit because technology is such an integral—and yet, at times invisible—aspect of contemporary law practice."[38] To make the duty explicit, the ABA amended the Model Rule 1.1 commentary language, which now explicitly reads that "[t]o 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*."[39] Practically speaking, "[t]his provision will require lawyers to better understand any advances in technology that genuinely relate to competent performance of the lawyer's duties to a client."[40]

Lawyers should not view this new language as a burden. Rather, the amended language reflects the "dual role" that lawyers must play in promoting effective data security throughout society, including for their own law practice and for their clients' businesses.[41]

---

[35] MODEL RULES OF PROF'L CONDUCT R. 1.1.

[36] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 6 (pre-2012 amendment). This language is now in cmt. 8 of ABA Model Rule 1.1.

[37] Resolution 105A, AMERICAN BAR ASS'N, 9 (Aug. 6-7, 2012) [hereinafter ABA Resolution 105A], *available at* http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105a.doc.

[38] *Id.* at 9.

[39] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (as amended) (emphasis added).

[40] Barkett, *supra* note 33, at 2-3.

[41] *See* LECLAIR & KEELEY, *supra* note 5, at 126 (explaining that this dual role reflects both that "a lawyer's competence includes understanding technology well enough to protect confidential client information," and that "a lawyer must understand technology and the law well enough to properly advise clients on how to satisfy legal

Lawyers should note the ongoing, diligent action necessary to fulfill the duty explicitly imposed by this new language. *The ABA Cybersecurity Handbook* acknowledges this significance by explaining that "a lawyer's ethical obligation of competence requires that the lawyer become and remain competent about the technology they use so as to be able to protect client confidential information."[42] In addition, the obligation "requires continued vigilance and learning as technology advances, in order to comply with a lawyer's duties under ethics rules."[43] It is also important to acknowledge that this obligation may even require getting outside help from experts, when needed.[44] According to *The ABA Cybersecurity Handbook*, "[i]f a lawyer is not competent to decide whether use of a particular technology (e.g., cloud storage, public Wi-Fi) allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer."[45]

When practicing and advising a client on data security issues, a lawyer must understand more than the technology they and their clients use. ABA Model Rule 2.1 explains that, "[i]n representing a client, a lawyer shall exercise independent professional judgment and render candid advice," which may involve referring "not only to law but to other considerations such as moral, economic, social and political factors, that

requirements and protect information and information systems"). "Cybersecurity . . . should not just be a concern of lawyers who practice 'cybersecurity law,' or who represent large technology corporations—it must be a concern of all members of the legal profession." *Id.* at 132. *The ABA Cybersecurity Handbook* explains that "the profusion of digital technologies has added cybersecurity to every client's primary interests, whether or not the client knows it, thereby drawing cybersecurity into the field of view that counsel must watch over if it is to provide competent representation of a client." ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 82.

[42] ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 65.

[43] *Id.* at 66.

[44] Ries, *supra* note 9, at 2 ("[Model Rule 1.1] requires attorneys who lack the necessary technical competence for security (many, if not most attorneys) to consult with qualified people who have the requisite expertise."); ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 66 ("Getting expert help is a recurring theme (as well as good advice) in ethics opinions on this subject.").

[45] ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 66.

may be relevant to the client's situation."[46] In the age of surveillance and hackers, there is no shortage of such issues to consider.

B. Confidentiality

Threats to data security also implicate another key tenet of a lawyer's ethical responsibilities: confidentiality. Most states' rules explain that, with limited exceptions, "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent."[47] *The ABA Cybersecurity Handbook* notes that "[t]his obligation to maintain confidentiality of all information concerning a client's representation, no matter the source, is paramount," and "is no less applicable to electronically stored information than to information contained in paper documents or not reduced to any written or stored form."[48] In many ways, confidentiality is at the "core" of a lawyer's ethical obligations when it comes to using new technologies.[49] It should be noted, however, that the current black letter rule, in most states, expresses only a negative obligation—the lawyer must refrain from doing something: revealing information.[50]

In order to understand the positive obligations of lawyers in this context, one must currently look to the commentary of the rule, which explains, "[a] lawyer [must] act competently to safeguard information relating to the representation of a client . . . against inadvertent or unauthorized disclosure."[51] This duty takes on increased significance with every new piece of technology a lawyer adopts in their practice.[52] In addition, commentary to the rule reads, "[w]hen transmitting a communication that includes information relating to the representation

[46] MODEL RULES OF PROF'L CONDUCT R. 2.1 (2012).

[47] MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2012).

[48] ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 62.

[49] Ries, *supra* note 9, at 1.

[50] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2012).

[51] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16 (pre-2012 amendments). This language now appears in cmt. 18 of ABA Model Rule 1.6.

[52] *See* Barkett, *supra* note 33, at 3 ("Laptops, thumb drives, anti-hacking security tools, search technology, among others, are related to protecting client-confidential information from inadvertent disclosure.").

of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[53] However, no special security measures are required, absent special circumstances, if the communication method affords a "reasonable expectation of privacy," which is determined by "the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement."[54]

In adopting the 2012 amendments, the ABA essentially decided the positive obligation to safeguard information, previously only described in the commentary, should appear more prominently in the actual rule. Despite the fact that "[t]his revision merely confirms the law under the ethics rules of every American Jurisdiction,"[55] the ABA resolution explained that "technological change has so enhanced the importance of this duty that it should be identified in the black letter and described in more detail in [the commentary]."[56] As a result, the new ABA Model Rule 1.6 Part (c) now explicitly states, "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."[57] In addition, and perhaps most significantly, Comment 18 now elaborates that the "[f]actors to be considered in determining the reasonableness of the lawyer's efforts" include

> the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards,

---

[53] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (pre-2012 amendments). This language now appears in cmt. 19 of ABA Model Rule 1.6.

[54] *Id.*

[55] ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 62. Prior to the adoption of the amended ABA Rules, the key professional responsibility requirements expressed in state ethics opinions had been described as requiring "competent and reasonable measures to safeguard client data, including an understanding of limitations in attorneys' competence, obtaining appropriate assistance, continuing security awareness, and ongoing review as technology, threats, and available security evolve over time." Ries, *supra* note 9, at 3. The revised rules have been characterized as "clarifications rather than substantive changes," which "add additional detail that is consistent with the [previous] rules and comments, ethics opinions, and generally accepted information security principles." *Id.* at 4.

[56] Resolution 105A, *supra* note 37, at 8.

[57] MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (as amended).

> 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).[58]

The significance of this change and the new standard it imposes upon lawyers has been widely noted.[59]

Most states' rules regarding confidentiality include commentary explaining that "[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."[60] Therefore, it is important for lawyers to have candid conversations with their clients in which they discuss their practice's use of technology and the associated risks. Lawyers are also obligated to have such conversations with clients under Model Rule 1.4, which requires appropriate communication with clients "about the means by which the client's objectives are to be accomplished."[61] This obligation includes communicating the ways in which the practice utilizes technology.[62] This rule also requires providing notice to clients when confidential information has been compromised.[63]

Practically speaking, these rules could empower clients to serve as a valuable check on the data security practices of law firms.[64] Clients are likely to embrace this role, as it is already evident they are becoming

---

[58] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18 (as amended).

[59] *See, e.g.*, Will Harrelson, *Mobile Device security for Lawyers: How Solos and Small Firms Can Ethically Allow Bring Your Own Device*, CURO LEGAL (June 24, 2014), http://www.curolegal.com/mobile-device-security-lawyers-solos-small-firms-can-ethically-allow-bring-your-own-device ("This is a monumental change that sets a new standard suggesting that lawyers are required to implement reasonable technological safeguards to prevent even an 'inadvertent' disclosure of a client's information or data.").

[60] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 19 (as amended).

[61] MODEL RULES OF PROF'L CONDUCT R. 1.4.

[62] Ries, *supra* note 9, at 2.

[63] *Id.*

[64] *See* Garrie, *supra* note 12 ("[A]ny company should require counsel to demonstrate that the law firm knows how to securely hold and manage an organization's data. This is particularly true in cases involving technology, trade secrets, or sensitive corporate data.").

more concerned with their firms' data security practices. In 2014, the New York Times reported that "companies are asking law firms to stop putting files on portable thumb drives, emailing them to nonsecure iPads or working on computers linked to a shared network in countries like China and Russia where hacking is prevalent."[65] Additionally, "banks and companies are threatening to withhold legal work from law firms that balk at the increased scrutiny or requesting that firms add insurance coverage for data breaches to their malpractice policies."[66] Despite the importance of enforcement from state ethics boards, "the push from corporate clients may have more impact on changing law firm attitudes than anything else."[67] This will only work if lawyers are open and honest with their clients about their use of technology[68] and if the legal profession as a whole encourages such practices. Listening to clients and embracing data security will not only ensure that firms are in compliance with ethics rules but may even provide a competitive an advantage in the legal marketplace.[69]

Finally, when discussing confidentiality, it is always important to remember that ABA Model Rule 1.9(c) and the corresponding rule in most states explains that confidentiality extends to the data of former clients.[70] This obligation is especially important in the context of data security, as electronic data storage is increasingly convenient and cost efficient, and enables lawyers to save large amounts of information pertaining to past cases for long periods of time.

When it comes to specific security measures that lawyers should adopt in light of their duty of confidentiality, lawyers should consider industry best practices, opinions from state ethics boards, and their client's preferences. For example, the State Bar of Arizona in 2009 issued an

---

[65] Goldstein, *supra* note 12.

[66] *Id.*

[67] *Id.*

[68] *See* Garrie, *supra* note 12 ("Unlike the physical structure of a bank, the level of information security readiness and effectiveness is not readily apparent to law firm clients, especially to those that are not technically skilled.").

[69] *See id.* ("[L]aw firms who know how to manage and secure technological assets should use that competitive advantage in marketing themselves to existing and potential clients.").

[70] MODEL RULES OF PROF'L CONDUCT R. 1.9(c).

opinion stating that, "[i]n satisfying the duty to take reasonable security precautions, lawyers should consider firewalls, password protection schemes, encryption, anti-virus measures," and other related measures.[71] However, a common caveat associated with lists of specific "reasonable security measurements" is that what constitutes "reasonable" will change over time. Indeed, states should avoid establishing "safe harbors" for lawyers or firms who satisfy minimum security requirements, which become quickly outdated. In this spirit, the Arizona opinion noted that "competent personnel should conduct periodic reviews to ensure that security precautions in place remain reasonable as technology progresses."[72]

At the end of the day, specific illustrative requirements might be helpful in guiding lawyers but should not be considered sufficient to protect their data. In short, "[l]awyers should be mindful of specific precautionary requirements within their jurisdiction, but should also realize that compliance with minimum standards of any kind—including those delineated in ethics rules—should only be a starting point for effective cybersecurity practice," and "[l]awyers should consider ways in which extra security measures can be employed where appropriate and feasible."[73]

C. Supervising Third Parties

In addition to making sure a lawyer's use of technology is ethical from a competence and confidentiality standpoint, legal ethics rules require lawyers to supervise the conduct of the other lawyers and non-lawyers inside and outside of the practice. This obligation stems from two rules that apply to law firm partners, as well as any lawyer "who individually or together with other lawyers possesses comparable managerial authority in a law firm."[74] Under the rules, such lawyers "shall make reasonable

[71] State Bar of Ariz. Ethics Opinions, 09-04: Confidentiality; Maintaining Client Files; Electronic Storage; Internet (Dec. 2009), *available at* http://www.azbar.org/Ethics/EthicsOpinions/ViewEthicsOpinion?id=704.

[72] *Id.*

[73] LECLAIR & KEELEY, *supra* note 5, at 125.

[74] MODEL RULES OF PROF'L CONDUCT R. 5.1 (2012).

efforts to ensure that the firm has in effect measures giving reasonable assurance that," first, "all lawyers in the firm conform to the Rules of Professional Conduct,"[75] and second, that the conduct of non-lawyers employed by, retained by, or associated with the lawyer, "is compatible with the professional obligations of the lawyer."[76]

These rules reflect the notion that a law firm's data security practices are only as strong as its weakest link. As a result, lawyers must make sure that subordinate attorneys, interns, paralegals, case managers, administrative assistants, and external business partners all understand necessary data security practices and the critical role that all parties play in ensuring the protection of client information.[77]

But modern lawyers are no longer only seeking outside help from *people*. For this reason, the ABA, in its 2012 review of the Model Rules, determined that the title of Model Rule 5.3, which is still the title of most states' rule on the subject, "Responsibilities Regarding Nonlawyer *Assistants*,"[78] is insufficient and misleading. The title now more appropriately and broadly reflects "Responsibilities Regarding Nonlawyer *Assistance*,"[79] implying more than just people. In addition, "[t]o reflect the scope of the nonlawyer services now being provided outside of firms,"[80] Model Rule 5.3's commentary now references "cloud computing" as an example of such modern practices.[81]

---

[75] *Id.*

[76] MODEL RULES OF PROF'L CONDUCT R. 5.3 (2012).

[77] *See* Garrie, *supra* note 12 ("Often the weakest link is not the technology, but the people, so it is essential firms make sure ingrained in every employee's mind is the need to be security aware."); *see also* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 111 ("Each professional at a law firm, and every administrative staff member, must be impressed with the personal responsibility that he or she owes to the firm's clients and partners with regard to information security.").

[78] MODEL RULES OF PROF'L CONDUCT R. 5.3 (pre-2012 amendments) (emphasis added).

[79] MODEL RULES OF PROF'L CONDUCT R. 5.3 (as amended) (emphasis added).

[80] Resolution 105C, AMERICAN BAR ASS'N, 7 (Aug. 6-7, 2012) *available at* http://www.americanbar.org/content/dam/aba/directories/policy/2012_hod_annual_meeting_105c.doc.

[81] MODEL RULES OF PROF'L CONDUCT R. 5.3 cmt. 3 (as amended).

Lawyers' use of cloud computing[82] has been the subject of various ethics opinions around the country and serves as a valuable example of how ethics boards treat the use of new technologies by lawyers.[83] A New Hampshire Bar opinion, for example, has led to the understanding that a cloud service provider "is 'in effect' a non-lawyer retained by the lawyer," invoking Rule 5.3.[84] Overall, states have generally ruled that cloud computing is permissible, as long as lawyers take proper steps when selecting and using services.[85] For example, in 2013, an Ohio opinion acknowledged that lawyers may use cloud services as long as they competently select an appropriate vendor, preserve confidentiality, safeguard client property, provide reasonable supervision of cloud vendors, and communicate with the client as appropriate.[86] However, Adam Cohen of Ernst & Young warns that, in some states, "[o]ther security measures more loudly demand that the lawyer augment his

---

[82] *The ABA Cybersecurity Handbook* defines cloud computing as "any system whereby a lawyer stores digital information on servers or systems that are not under the close control of the lawyer or the lawyer's firm." ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 77. More colloquially, the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility describes it as "merely 'a fancy way of saying stuff's not on your [own] computer.'" Pa. Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility Formal Op. 2011-200 at 1 (citing Quinn Norton, "Byte Rights," *Maximum PC*, Sept. 2010, at 12).

[83] The ABA provides an online guide to "Cloud Ethics Opinions Around the U.S." *Cloud Ethics Opinions Around the U.S.*, AMERICAN BAR ASS'N, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited May 23, 2015). In addition, *The ABA Cybersecurity Handbook* contains an appendix of "Ethics Opinions on Lawyer Confidentiality Obligations Concerning Cloud Computing." ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 245.

[84] *See* Barkett, *supra* note 33, at 9 (citing N.H. Bar Ethics Op. #2012-13/4).

[85] *See* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 78 (explaining that state ethics opinions "make clear that a lawyer must have a basic understanding of the technical aspects of cloud computing, and should conduct a due diligence evaluation of the provider to ensure that they have adequate security measures").

[86] *Cloud Ethics Opinions Around the U.S.*, *supra* note 83 (citing OSBA Informal Advisory Op. 2013-03, *available at* https://www.ohiobar.org/ForPublic/LegalTools/Documents/OSBAInfAdvOp2013-03.pdf). Some states provide more specific requirements. For example, Maine lists seven requirements "the attorney should ensure that the vendor of cloud computing services or hardware" follows. Me. Bd. of Bar Overseers Op. #207: The Ethics of Cloud Computing and Storage (Jan. 8, 2013), *available at* http://www.maine.gov/tools/whatsnew/index.php?topic=mebar_overseers_ethics_opinions&id=478397&v=article.

efforts with expert technical assistance."[87] Measures that may require outside help include, among others, Iowa's requirement to "[d]etermine the degree of protection the vendor provides to its clients' data," New Jersey's requirement to "[m]ake sure that vendors are using available technology to guard against foreseeable infiltration attempts," and North Carolina's requirement to "[e]valuate the vendor's security and backup strategy."[88] *The ABA Cybersecurity Handbook* wisely acknowledges that "rapidly evolving technology means that these factors cannot provide a 'safe harbor.'"[89] Instead, "[l]awyers should monitor and reassess the protections of the cloud provider as the technology evolves."[90]

It is also worth noting the limits of a lawyer's duties under the rules. As the New Hampshire Bar has explained, "a lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology," and "[w]hen it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard."[91]

III. Promoting Our Individual and Collective Obligation to Protect Client Data

These ethics rules establish an undeniable obligation for all attorneys to take affirmative steps to protect client information while practicing law in the age of hackers. In order to achieve the ultimate goal of improved data security practices of lawyers and their clients, it would behoove the legal profession to view this obligation as a collective one.

---

[87] Adam Cohen, *Lawyers Between a Rock (Social Media) and a Hard Place (The Cloud)*, INSIDE COUNSEL (Apr. 16, 2014), http://www.insidecounsel.com/2014/04/16/lawyers-between-a-rock-social-media-and-a-hard-pla.

[88] *Id.* ("Lawyers aiming to achieve this level of diligence will have to learn some basics about network security defenses such as firewalls, intrusion detection systems and patches, as well as physical or environmental security for data centers. It is probably safe to say that this subject matter does not form part of the curriculum at law schools, which strongly suggests that resort to technical experts is prudent.").

[89] ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 77.

[90] *Id.*

[91] Barkett, *supra* note 33, at 10 (quoting N.H. Bar Ethics Op. #2012-13/4).

When it comes to data security, it is up to the profession as a whole to ensure that relevant legal ethics rules are properly promoted and enforced. This obligation will require education—early and often—as well as continued awareness and diligent enforcement.

A. Educating Lawyers From the Beginning —Law Schools

The responsibility of law schools in this effort is two-fold: educating law students how to responsibly use technology in practice[92] and educating them about the ethical implications of not doing so.[93] For different reasons, this responsibility will be challenging for both instructors and students.

In addition to the obvious challenges that result from the generational gap between veteran lawyers and law students, many law professors have the disadvantage of not having practiced law in the age of hackers.[94] The topic may prove to be even more challenging for younger, complacent law students who think they already know everything there is to know about technology.[95] This complacency, however, should not dissuade professors or students from understanding the relevant ethical considerations and the care that must go into the responsible use of technology

---

[92] *See* Catherine J. Lanctot, *Becoming a Competent 21st Century Legal Ethics Professor: Everything You Always Wanted to Know About Technology (But Were Afraid to Ask)*, J. OF THE PROF'L LAW. (forthcoming 2015), at 12 (citing commentators that "have cautioned that failure to prepare today's law students for the challenges of using technology in the practice of law does them a grave disservice").

[93] *Id.* at 13 ("[T]he ethical use of modern technology should be an integral part of the curriculum at all American law schools.").

[94] *Id.* at 2 ("Law professors may be even less comfortable with the developments of the Digital Age than practitioners.").

[95] *See* Kristin J. Hazelwood, *Technology and Client Communications: Preparing Law Students and New Lawyers to Make Choices That Comply with the Ethical Duties of Confidentiality, Competence, and Communications*, 83 MISS. L.J. 245, 280 (2014) (footnote ommitted) ("[E]valuation of the benefits and risks of technology is perhaps most challenging for the current generation of law students and new lawyers, who are primarily part of the technologically-inclined Millennial Generation."). Indeed, "the current generation of law students is the first generation to have grown up using technology." *Id.* at 283 (footnote omitted).

throughout their legal careers.[96] At the end of the day, "students' familiarity with technology necessitates perhaps a different approach to instruction about its use, but does not vitiate the necessity of that instruction."[97]

The role of legal ethics in data security should be taught across all courses: subject-specific, legal research and writing, and ethics.

In this day and age, when it comes to traditional subject-specific courses, the implications of technology on the law are bound to come up naturally in a wide array of contexts. Such occurrences should be seized as opportunities to also discuss the ethical implications of data security in the practice of law. The risks associated with technology can also be incorporated, along with legal ethics, into legal research and writing courses.[98]

However, sporadic, convenient references, without more, should not be seen as sufficient to fully address the myriad ethical implications that arise when it comes to data security in the legal profession. As one professor noted,

> Of course, the dramatic effect that the Internet and digital technologies have had on every area of the law has produced changes in the substantive material we cover in our classes. But it is less certain that our current approach to teaching legal ethics adequately reflects the ongoing technological upheaval in the legal profession.[99]

These issues should warrant prominent coverage within the law school curriculum. Therefore, the easiest and best way to address the legal ethics implications of data security would be to devote substantial attention to

---

[96] *See* Lanctot, *supra* note 92, at 50 ("[L]awyers who will be successful in riding the next waves of technological disruption will be the ones who maintain a skepticism and cautious approach to each shiny new object that is dangled before them.").

[97] Hazelwood, *supra* note 95, at 283 (footnote omitted).

[98] *Id.* at 280 ("[T]his Article proposes that law professors, legal writing professors in particular, and lawyers who supervise new lawyers challenge law students and new lawyers to think critically about when and how they use technology to communicate confidential client information so that they are adequately prepared to represent their clients.").

[99] Lanctot, *supra* note 92, at 2.

the topic in a "professional responsibility" or "legal ethics" course.[100] Only through these courses will law schools be able to fully devote the necessary attention to the practical, ethical challenges lawyers face with regard to data security in practice today, while also keeping an eye to the uncertain challenges of the future.[101]

B. Educating Employees

Education about data security and ethics should not end when a lawyer graduates law school; it must be a career-long commitment that is embraced by both employees and employers within the legal profession. Accordingly, addressing data security requirements within a firm requires more than assigning tasks to the Information Technology (IT) department. Indeed, "[m]any attorneys incorrectly think that security is for the IT department or consultants. While IT has a critical role, everyone, including management, all attorneys, and all support personnel, must be involved for effective security."[102] Proper and ethical supervision of subordinate lawyers, other firm staff, and business partners, means properly educating all parties about legal ethics in the age of hackers, and what it takes to comply with specific rules. Such actions are not only ethically required, they are desperately needed within the profession and must be taken seriously. The *Wall Street Journal* reported that "the weakest links at law firms of any size are often their own employees, including lawyers."[103] At the end of the day, "lawyers are responsible for their staff—their ethical violations are the lawyer's ethical violations."[104] From this standpoint, an appropriate goal is to create a "culture

---

[100] *Id.* at 13 ("Incorporating current issues about technology into our legal ethics classes can be done without wholesale revision of our courses, and without taking a crash course in Computer Programming 101." (citing Simon Canick, *Infusing Technology Skills Into The Law School Curriculum*, 42 CAP. U. L. REV. 663 (2014))).

[101] *Id.* at 49 ("[A]t the end of a modern twenty-first century course in legal ethics, law students must be prepared to practice law in that future environment that we may only dimly anticipate today.").

[102] Ries, *supra* note 9, at 4-5.

[103] Jennifer Smith, *Lawyers Get Vigilant on Cybersecurity*, WALL ST. J. (June 26, 2012), http://www.wsj.com/articles/SB10001424052702304586045774867611017 26748.

[104] LECLAIR & KEELEY, *supra* note 5, at 136.

of security,"[105] both within law firms and within the profession as a whole.

In these efforts, it is especially important to educate young employees, with whom "instruction is crucial because law students' and new lawyers' comfort with technology perhaps makes it more difficult for them to anticipate risks associated with it, which ethics opinions and the Model Rules require."[106] The profession cannot just rely on the new generation of lawyers to pick up the slack when it comes to data security; young lawyers are just as much in need of data security training as veteran lawyers.[107] Although lawyers cannot entirely pass off problems to IT experts, the profession must acknowledge the need for expert help when it is necessary.[108] Finally, lawyers must remember that supervising third parties also includes educating entities with which they contract, as "it can be said that the security of a law firm is only as strong as that of its weakest business partner."[109]

C. Bar Associations and Ethics Bodies

Bar associations and state ethics bodies are in a position to promote the importance of data security by providing resources, training, and

---

[105] *See* International Legal Technology Ass'n, *Risks and Rewards: The Good, the Bad, and the Revered* (Oct. 2013), at 28, http://epubs.iltanet.org/i/192213 ("The best defense against internal and external threats is to create a culture of security that focuses on the human element and changes behavior to help safeguard information. To build an effective security culture in your firm, it's necessary to move beyond technical safeguards and policies, focusing on the firm's employees—attorneys and staff.").

[106] Hazelwood, *supra* note 95, at 248.

[107] *See id.* at 281 (citing Kendra Huard Fershee, *The New Legal Writing: The Importance of Teaching Law Students How to Use e-mail Professionally*, 71 MD. L. REV. Endnotes 1, 10-14 (2012) ("That the current generation of law students and new lawyers are part of the technologically savvy Millennial Generation does not lessen the need for instruction regarding electronic communication.").

[108] *See* Renato Pontello, *BYOD: Going Beyond Your IT Policy*, CANADIAN LAWYER MAG. (Aug. 19, 2013), http://www.canadianlawyermag.com/4780/BYOD-going-beyond-your-IT-policy.html ("If the skillset does not exist in your legal department, it should be developed, recruited, or outsourced.").

[109] ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 25.

continuing legal education courses (CLEs) and by updating state ethics rules to increase awareness and enforcement of data security obligations.

1. Providing Resources

The ABA has shown tremendous leadership and pro-activeness in addressing these data security and ethics issues over the last few years. In August of 2012, the ABA Board of Governors created the Cybersecurity Legal Task Force, which coordinated many great efforts to guide attorneys with educational materials,[110] including the frequently cited *ABA Cybersecurity Handbook*.[111] The ABA's online Legal Technology Resource Center provides helpful resources for attorneys, such as the guide to "Cloud Ethics Opinions Around the U.S."[112] The ABA Center for Professional Responsibility also provides a host of helpful resources for the applicable Model Rules, as well as providing state-specific resources.[113] State and local bar associations should follow suit by linking to these resources and providing their own.

2. Training and CLE

Bar associations must realize that, by nature, all lawyers are prone to exacerbating the data security risks associated with technology use. As one Canadian lawyer explained, legal departments "are as guilty as anyone in society (and arguably more so) of falling prey to a kind of technological somnambulism where, enamoured by the marvels of today's digital technology, we have not thought deeply enough . . . about the long-term implications of how its use is materially impacting corporate behaviour (i.e. decision-making, allocation, and mitigation of risk, etc.)."[114] It is also important to remember "attorneys are consumers

---

[110] *See* Podgers, *supra* note 10.

[111] *See generally* ABA CYBERSECURITY HANDBOOK, *supra* note 3.

[112] *Cloud Ethics Opinions Around the U.S.*, *supra* note 83.

[113] Center for Professional Responsibility, *Resources*, AMERICAN BAR ASS'N, http://www.americanbar.org/groups/professional_responsibility/resources.html (last visited May 23, 2015).

[114] Pontello, *supra* note 108.

too. They are not immune to media hype and the desire to appear trendy or a few steps ahead of their peers when it comes to technology."[115]

Given these tendencies when it comes to using potentially vulnerable technology within the legal profession, bar associations can provide a tremendous service to lawyers by offering training and CLEs on proper data security compliance with the relevant ethics rules. Although some lawyers are hopefully receiving training from inside their firm, many small or solo practices, in addition to lawyers in the government and public interest settings, may not have the resources to effectively educate employees on these issues.[116]

Even for those lawyers that are committed to learning and implementing effective data security practices, "[t]he greatest challenge for lawyers in establishing cyber security programs is deciding what security measures are necessary and then implementing them."[117] Bar-sponsored trainings and CLEs can go a long way toward educating lawyers, who will then be better fit not only to ethically practice, but also to train other employees. At its 2014 Annual Meeting in Boston, the ABA and its Center for Professional Responsibility offered a CLE entitled "The Low Tech Lawyer's Guide to Ethical Competence in a Digital Age."[118] State and local bar associations should follow suit with similar programming.

---

[115] *Adapting to a Mobile World*, INTERNATIONAL LEGAL TECHNOLOGY ASS'N, http://www.iltanet.org/MainMenuCategory/Publications/WhitePapersandSurveys/Adapting-to-a-Mobile-World.html (last visited May 10, 2015).

[116] *See* Jennifer Smith, *Client Secrets at Risk as Hackers Target Law Firms*, WALL ST. J. LAW BLOG (June 25, 2012), http://blogs.wsj.com/law/2012/06/25/dont-click-on-that-link-client-secrets-at-risk-as-hackers-target-law-firms ("The challenge is protecting the data . . . the smaller the firm gets, the more difficult it gets for them to put the proper controls and to educate the firm." (quoting Carlos Rodriguez, manager of network infrastructure and security for the Midwestern law firm Lathrop & Gage LLP)).

[117] Ries, *supra* note 9.

[118] James Podgers, *You Don't Need Perfect Tech Knowhow for Ethics' Sake—But a Reasonable Grasp Is Essential*, ABA J. (Aug. 9, 2014), http://www.abajournal.com/news/article/you_dont_need_perfect_tech_knowhow_for_ethics_sake--but_a_reasonable_grasp.

3. Updating, Promoting, and Enforcing Ethics Rules

A final way to ensure that lawyers pay more attention to cyber-attacks and threats to their confidential client information is for states to adopt the ABA's updated rules, which clearly, prominently, and forcefully explain a lawyer's obligations in the age of hackers. Adopting the updated rules would significantly lessen the burden on lawyers who want to practice ethically but are not inclined to explore model rules and opinions from outside their jurisdiction for guidance.[119] Several states have already adopted some or all of the ABA's 2012 amendments,[120] with more expected to follow in the coming years.[121] Clients are counting on bar associations and ethics bodies to continue to fulfill this critical role of helping lawyers prevent breaches of their confidential information.[122]

Conclusion

The threat of cyber-attacks on law firms is great and likely more serious than the profession realizes due to the disincentives to publically

---

[119] *See* Podgers, *supra* note 10 ("The threat to confidential client information from cyberattacks raises ethics concerns that require more attention from lawyers .... That could change, however, as states begin to consider adopting revisions to the ABA Model Rules of Professional Conduct that were adopted by the association's policymaking House of Delegates in August [2012] at the recommendation of the Commission on Ethics 20/20.").

[120] *See* American Bar Association Center for Professional Responsibility Policy Implementation Committee, *Chronological List of States Adopting Amendments to their Rules of Professional Conduct Based Upon the August 2012 Policies of the ABA Commission on Ethics 20/20*, AMERICAN BAR ASS'N (Mar. 16, 2014), http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/chron_adoption_e_20_20_amendments.authcheckdam.pdf.

[121] *See* Barkett, *supra* note 33, at 4 ("Now that these changes have been adopted by the ABA House of Delegates, they will slowly be incorporated into State rules of professional conduct.").

[122] *See* Lea L. Lach, *Throwing New Flags: Should There Be Criminal Sanctions or a Better Chance of Civil Sanctions for Lawyers or Service Providers Who Breach Confidentiality?*, 14 U. PITT. J. TECH. L. & POL'Y 315, 332 ("For the time being, clients must trust state bar associations to help lawyers prevent breach of confidentiality in the cloud and to impose sanctions for it. Fortunately, bar associations seem well prepared to do so in light of their experience with earlier storage methods that posed a threat to confidentiality.").

acknowledge breaches and share information.[123] Nevertheless, lawyers and law firms have ethical obligations to take reasonable affirmative steps to protect confidential client information. Some of the necessary compliance steps might seem burdensome,[124] but hiding from threats to data is not an option.[125] It is practical and reasonable for firms to stay educated, to create a "security-aware culture," and to seek outside help when needed.[126] After all, "[t]he requirement for lawyers is reasonable security, not absolute security."[127]

The challenges of practicing law in the age of hackers are great, but the goal of protecting both confidential client information and law firm data is an attainable one.[128] It is incumbent upon the profession as a whole to embrace the reality that "lawyers must confront [these] challenges by staying abreast of technology, monitoring applicable ethics opinions and court decisions, and knowing the rules applicable in their jurisdiction."[129] Embracing this reality through awareness of ethical obligations and education regarding technology and data security will

---

[123] *See* Smith, *supra* note 116 ("The FBI doesn't keep statistics on law firm cyberattacks, and few firms are willing to publicly disclose a breach for fear of damaging their reputations.").

[124] *See* Garrie, *supra* note 12 ("For many firms, hiring world class security engineers to work full time is seen as impractical. And, acquiring the right hardware and software solutions is too costly.").

[125] *See* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 64 ("In short, a lawyer cannot take the 'ostrich' approach of hiding his head in the sand and hoping that his office or firm will not suffer a data breach that compromises client information. [Instead, l]awyers must implement administrative, technical, and physical safeguards to meet their obligation to make reasonable efforts to protect client information.").

[126] *See* Garrie, *supra* note 12 ("While investing millions is not practical, if the law firm has a security-aware culture and has purchased and implemented one of the current solutions available in the marketplace, it can provide a secure and easy-to-use file transfer solution, a highly advanced email encryption service, an integrated malicious-code-detector for both the Internet connection and physical devices, a solution that manages and protects data in transit between mission critical system and security platforms, and technology that provides network protection from all outside threats.").

[127] Ries, *supra* note 9.

[128] *See* ABA CYBERSECURITY HANDBOOK, *supra* note 3, at 32 ("Is Protecting the Privacy and Security of Confidential and Sensitive Law Firm Records and Attainable Goal?").

[129] Barkett, *supra* note 33, at 21.

help ensure a future in which clients can continue to depend on the legal profession to provide competent, confidential legal services. Technologies "have made legal practice more difficult in some ways, and provided opportunities in others. Whether the difficulties or the opportunities tip the balance is up to the lawyer, but knowledge, acquired or borrowed, can only work in favor of success."[130] Like all sectors, there will never be a perfectly secure legal profession; but with proper awareness, motivation, and guidance, lawyers can confidently, responsibly, and ethically practice law in the age of hackers.

[130] Cohen, *supra* note 87.

Aon Risk Solutions
Speciality | Professional Services

Ten Cybersecurity Strategies for Law Firms

How to develop an appropriate cybersecurity plan

September 2014

Risk. Reinsurance. Human Resources.

AON
Empower Results®

Table of Contents

Introduction

Potential data breaches and cyber-attacks are an unfortunate reality for good law firms. The external threat environment continues to evolve, steered by criminal hackers (organized crime), "hacktivists" who want to embarrass firms or their clients as opposed to seeking information for monetary gain, and state-sponsored hackers in countries such as China, Iran, Syria, North Korea, and Russia. In actuality, however, the greatest threats to law firms are the internal ones posed by a firm's lawyers and staff. While malicious insiders—such as dishonest employees who gain access to sensitive client data in furtherance of insider trading schemes—cannot be ignored, lawyers and staff who negligently open holes on the firm's IT security network are more common culprits. These innocent breaches are usually caused by employees losing laptops or mobile devices containing sensitive data, opening spear phishing emails or other suspicious attachments, or using easy-to-crack passwords for all of their devices.

Given this landscape, law firms must adopt pragmatic information security practices and procedures to reduce the risk of liability and reputational injury. Lawyers must also protect client information to respect their ethical obligations. Model Rule of Professional Conduct 1.6(c) (2014) specifically requires lawyers "to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Comment 8 to Model Rule 1.1 emphasizes that meaningful awareness of changes in relevant technology is now an integral aspect of lawyers' duty of competence.

Recognizing that there is abundant literature on cyber security issues, this short overview is intended to help firms that are in the process of developing related processes, policies, and programs grasp key issues that may affect their planning. The strategies that follow are not intended to establish best-practices standards for law firms, nor are any of them intended to reflect a standard of care in professional liability litigation. Rather, we offer these strategies as a starting point for law firms that are working toward adopting practices and procedures meeting their specific needs. Not all of the steps outlined here will fit all firms. We further realize that some of the strategies provided here may initially appear to be excessive and have little to do with normal law firm operations. We are sympathetic to related frustrations, but the information security requirements imposed by some federal and state laws, such as HIPAA, are expansive. The result, naturally, is the creation of associated burdens on law firms and other organizations that are subject to those laws. On a positive note, law firms with reasonable IT security processes and standard human resources practices probably are already implementing many of these strategies. In short, a law firm should take steps to achieve its information security goals based on what is reasonable and appropriate for the firm's individual circumstances.

Douglas R. Richmond
Managing Director
Professional Services
Aon Risk Solutions
doug.richmond@aon.com

Matthew K. Corbin
Vice President and Director
Professional Services
Aon Risk Solutions
matthew.corbin@aon.com

Ten Cybersecurity Strategies for Law Firms

I. **Assign cybersecurity roles and responsibilities for the entire law firm.**

A. Identify the key security stakeholders (e.g., managing partner, firm administrator, chief executive officer, chief financial officer, executive committee, technology committee, general counsel or loss prevention partner, practice group leaders, human resources, IT personnel, records staff, finance and accounting staff) and assemble an information security team and designate a team leader.

B. Clearly define team members' roles and responsibilities to ensure accountability.

II. **Conduct a risk assessment to analyze the firm's operational environment and obtain a clear view of the firm's vulnerabilities.**

A. To the extent reasonably possible, inventory the firm's physical equipment and devices (desktop computers, laptops, flash drives), and software systems and applications.

B. Identify the custodians and storage locations of the firm's data.

C. Create and maintain a data map, which is a chart that illustrates where data is stored in the firm and who is responsible for that data.

1. A data map should include data storage locations; individuals responsible for certain data; data flow (transmission and transportation); lifecycle (when a document was created and when it should be destroyed); and plans if a breach occurs.
2. As part of this process, track information collected from clients to understand who the information is collected from, where the information is stored, and who has (or may have) access to the information.

D. Perform a gap analysis. Once a firm understands how data flows through its systems, it can understand the risks to that information and determine the best way to manage the risks. The firm needs to identify the gap between the desired and current state, and close the gaps by developing a prioritized remediation plan.

III. **Employ a data classification system.**

A. Law firms should classify the information they collect and store the information according to its level of importance and sensitivity.

B. For each security classification level (e.g., public, internal use only, confidential, sensitive, non-sensitive, protected health information), the firm should identify the types of security controls and protections available for the data; who has access to the data and why; data ownership; and retention and destruction requirements. Importantly, a classification system should be easy for lawyers and staff to understand.

C. Data should be classified as it is saved on the firm's network.

IV. **Control and limit data access.**

A. Control and limit access to data to minimize scope of losses and establish a level of accountability.

B. To limit access, law firms can password-protect data; scan outbound email for attachments; scan data copied to removable drives and backup systems; and manage devices by encrypting and tracking them, and ensuring that they may be remotely wiped of data.

C. Firms should require lawyers to use only firm-issued flash drives and CDs when using firm computers. Those devices should always contain only firm documents or files.

D. There is debate about whether law firms should have "open" or "closed" records management systems, or whether a hybrid system (e.g., some matters or matters in a particular practice area are closed while others are not) is preferable. In a closed system, a firm limits access to documents collected or prepared in connection with a matter to only those law firm personnel who are working on the matter, or personnel authorized to be involved in the processing, hosting, review and production of data, such as litigation support personnel, e-discovery specialists, and system administrators. If another lawyer in the firm wants to view a document in a matter on which she is not working, she needs the permission of an authorized lawyer. Whether a law firm should have an open or closed system, or something in between, depends on the firm and its practices. Closed systems are the most secure.

E. When appropriate, conduct background checks on law school interns, summer clerks, temporary employees, contract employees, and support staff who may handle tasks with sensitive information.

F. Law firm personnel should not work on matters using their own mobile devices, personnel email accounts, or personal computers.

1. Some firms may have a "bring your own device" policy. While such a policy may help the firm lower costs (assuming the employees pay for the devices) and increase employee satisfaction, those benefits come at the cost of potential security breaches. At a minimum, employee-owned devices should be partitioned to segregate personal and firm data. It is also critical to erase all firm data on these devices when employees leave the firm.

G. Limit the delivery and exchange of client-related documents to secure channels. Encryption should be used for the transmission or delivery of personally identifiable information ("PII").

1. PII is any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

H. Properly dispose of information at the conclusion of a matter. In most cases, merely hitting "delete" on a file containing sensitive material is insufficient to actually remove the data from the network. The data still exists until other data overwrites it, leaving it vulnerable to recovery. To securely delete sensitive data, use software (such as Eraser) that will overwrite the space where the file once sat with random data. In addition, remember that data may still reside on the firm's copiers, scanners, or other equipment. Some state laws mandate how business records must be destroyed if they contain PII.

I. Establish policies to automatically revoke network access, including remote access, upon an employee's termination or resignation from the firm. Implement procedures to have messages sent to the employee's mailbox forwarded to a designated firm employee. When appropriate, a firm should utilize an exit process to gather all firm equipment (security cards, keys), confirm that the employee is leaving all data with the firm, and inform the employee that post-termination access is a criminal act.

V. **Establish information and data security policies and procedures, and regularly review and update them.**

A. Consider following a recognized information security framework to reflect the strength of the law firm's information security practices and procedures.

1. ISO 27001 is an internationally recognized, certifiable information security standard that provides a framework for protecting information and securing data and systems. Essentially, a firm is required to follow a standardized set of audit procedures which results in an independent and objective opinion that the firm manages its information security properly. It reduces the burden of proving compliance with multiple standards (HIPAA, state PII laws) by building a single standard for information security.

2. In February 2013, President Obama issued an executive order calling for the development of a set of existing standards, guidelines, and practices to help organizations manage cyber risks. As a result, on February 12, 2014, the National Institute of Standards and Technology ("NIST") released "Framework for Improving Critical Infrastructure Cybersecurity." The framework provides a structure that organizations can use to create, guide, assess, or improve cybersecurity programs. The NIST's framework is available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

3. COBIT 5 (control objectives for information and related technology) is a framework created by the Information Systems Audit and Control Association ("ISACA"), for information technology management and IT governance. COBIT is one of the most commonly used frameworks to comply with the Sarbanes-Oxley Act of 2002.

4. Law firms that fall within the definition of "business associate" under HIPAA must comply with the Privacy Rule, the Breach Notification Rule, and the Security Rule. Upon request, we can provide prototype policies for these three rules. While the prototype policies are intended to assist firms with establishing and maintaining a HIPAA security program, they also provide a general framework for developing information and data security policies and procedures. For instance, the Security Rule contains 18 standards and 36 implementation specifications addressing many of the strategies in this overview, such as risk analysis, access authorization, security training, transmission security, monitoring, facility security, and data back-up to just name a few.

B. Policies regarding the privacy and security of firm data should include the use of encryption, remote access, mobile devices, thumb drives, laptops, Wi-Fi hotspots, clouds, web email accounts, and social networking sites.

C. Make protocols for security monitoring a priority.

1. Monitor information system and assets at discrete intervals to identify potential cybersecurity threats and events, and to verify the effectiveness of the firm's protective measures.

2. Monitor the firm's physical environment to detect potential cybersecurity events.

3. Monitor for unauthorized personnel, connections, devices, and software.

4. Test the firm's detection processes to ensure awareness of irregular events.

VI. **Utilize protective technology and related procedures.**

A. Deploy data and disk encryption as much as possible, whether data is transmitted to others or stored on the firm's computers.

1. Laptops should be protected with whole disk encryption because lost laptops are one of the leading causes of data breaches.

2. Encrypt wireless routers.

B. In appropriate circumstances, segment the firm's network to create silos of information accessible on a need-to-know basis, i.e., stand-alone servers apart from the standard networks to store sensitive data. Some client's data may need to be compartmentalized or stored on a separate server with stronger security protections and stronger access controls.

C. Establish data logs (records of events created by a computer program) so that if a data breach occurs, a forensic investigator can determine the scope and cause of a data breach.

D. Use content scanner tools (i.e., file system crawlers) to notify an administrator if a document is not in the correct place, and to move, quarantine, or delete the file.

E. Back up important documents and files to protect data in the event of an operating system crash, hardware failure, or virus attack. Back-up information should be tested periodically.

F. Avoid software downloads from the internet.

G. Retain third-party consultants to conduct vulnerability scans, penetration tests, and malware scans.

H. Other generally accepted protective technology and security measures include: firewall protection; malware (malicious software) protection; password protection; identity-verification security questions; anti-virus software and virus scanners; regular installation of software updates and security patches; user activity monitoring; digital rights management; advanced threat and botnet protection; privilege access management; web and email content management; incident management reporting; network monitoring tools; two-factor authentication; remote wipe and data destruction; secure file transfer and transport lawyer security certificates; network monitoring tools; virtual private networks; and vulnerability scanning software.

VII. **Conduct information security awareness training for all firm personnel.**

A. A firm's policies are only as good as its practices. Provide cybersecurity awareness education for the entire firm. Firm management, as opposed to the IT department, must set the tone to instill a culture of information security.

B. Engage lawyers and staff with training sessions, email updates, etc.

C. Content and Curriculum for Security Awareness Training Programs

1. Strong Password Selection

a. A strong password uses a combination of length (at least eight characters) and different categories of characters (uppercase, lowercase, numbers, and symbols).

b. Avoid using common names, phrases, sports teams, pet names, etc.

c. Avoid making a password comprised of only numbers or only letters.

d. Do not repeat passwords.

e. Do not use a firm password as a personal account password.

f. Do not use a personal account password as a firm password.

g. Do not share passwords with family and friends.

2. Email Security Measures

    a. Separate personal email from work email. Personal and business email accounts should not be linked, or have similar usernames and passwords. Keep work emails separate and in their own account, and use personal email accounts for friends and family. Use separate passwords for business and personal accounts.

    b. Recognize spear phishing attacks (suspicious emails) by looking for spelling errors, poor formatting, references to accounts or to institutions with which the recipient has no connection or is unfamiliar, and threatened consequences of non-response, such as disabling accounts or the loss of benefits.

    c. Avoid clicking on random links or opening attachments from emails sent by unknown senders, emails that you were not expecting to receive, or emails with strange subject lines.

    d. Open any suspicious email, attachment, or link on a computer that is not connected to the firm's network.

3. Review procedures for backup (e.g., saving of data to network drives).

4. Review policies for reporting data breach incidents.

5. Review policies for downloading software or other outside applications on the firm's information system.

6. Review any "bring your own device" or remote access policies.

7. Review any social media policies.

8. Review policies for logging out of or locking a computer when stepping away from a work area.

9. Review policies for proper storage and extraction of data. Most vulnerable information is unknowingly shared using unsecured USB drives, SharePoint, cloud storage, and other repositories outside the firm's firewall.

10. Drive home the message that the firm's policies will be enforced.

VIII. Undertake due diligence when retaining third party service providers.

A. Check the credentials of third party vendors (payroll, virtual paralegals, virtual receptionists, data backup, case management, cloud computing).

B. Understand vendors' security processes and protocols.

    1. Know exactly where vendors will store firm data.

    2. Make sure vendors treat data consistent with the firm's security objectives. This includes investigating vendors' security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances.

    3. Investigate vendors' ability to purge and wipe copies of data, and to move data to a different host.

    4. Seek vendors that give comfort that data will be accessible when needed.

    5. Ensure not only that appropriate security measures are in place, but that they are continually upgraded to meet the evolving threats landscape.

C. Review—do not merely sign—the third party's terms and conditions of service.

IX. **Implement a data breach incident response plan.**

A. Train key management and personnel who will make up the incident response team (e.g., executive management, IT, general counsel or loss prevention partner, human resources, public relations). Specify each team member's responsibilities, and know who is in charge of the team.

B. Prepare an accurate system diagram, with data flow and infrastructure maps to show where the firm's data is located.

C. Know what is normal in the firm's environment. By establishing a baseline of network operations and expected data flow, a firm will improve its efforts to detect anomalies. Warning signs include spear phishing, malware quarantines, egress communications to strange IP addresses, and failed log-in attempts.

D. All attorneys and support staff should be trained to immediately notify the firm in the event of an actual or suspected breach.

E. Determine the scale and scope of the breach, i.e., what data has been exposed, and reduce further exposure through containment. If possible, isolate affected systems, or deactivate or discontinue services under attack.

F. Document everything before and after an incident.

1. Create a timeline of associated accounts and suspect files.
2. Encourage broad preservation and collection of evidence.
3. Do not analyze original evidence; analyze a copy if possible.
4. Destroy nothing.

G. For each firm office location, identify points of contact with law enforcement, internet service providers, forensic experts, and the communication companies that service the firm.

H. Urge careful use of wording, i.e., don't call it a breach until the person in charge of the incident response team calls it a breach.

I. Plan how the firm will conduct its business continuity operations and thereby reduce the impact of the event.

J. Determine if the data breach triggers any federal or state notification requirements. Reporting requirements depend upon the type of information and the scope of the breach.

1. Forty-six states impose reporting obligations in the event of a security breach.
2. Federal laws containing reporting obligations include the Health Insurance Portability and Accountability Act (HIPAA); Health Information Technology for Economic and Clinical Health Act (HITECH Act); Gramm-Leach-Bliley Act; Federal Trade Commission Act; and Fair Credit Reporting Act.
3. Even in the absence of a state or federal law, a lawyer has an ethical duty to inform clients of security incidents. More specifically, the duty to communicate under Model Rule 1.4 encompasses the duty to inform a client that its confidential information has been compromised. If timely informed of the breach, the client may be able to mitigate the damage. For instance, the client may have a better chance of identifying the perpetrator based on the client's knowledge of the particular industry or otherwise possess a greater ability to anticipate how the compromised information may be used.

K. Evaluate and update the plan at regular intervals.

L. Conduct tabletop exercises to rehearse for a data breach at regular intervals.

M. Following a data breach, review all documented activity in a roundtable environment and identify what procedures worked well and what areas need improvement.

X. **Consider purchasing cyber liability coverage.**

A. Depending on the facts, in the event of a breach a law firm could be covered under one or more of its existing insurance policies, including lawyers' professional liability, employment practices liability, fiduciary liability, and management liability. In addition, review a third party vendors' insurance policies for possible "additional insured" coverage under those policies.

B. Consider purchasing cyber liability coverage.[1] As a general rule, and again depending on the facts, cyber liability insurance is more likely to provide a firm with coverage in the event of a breach than are other forms of insurance that the firm may have in place.

C. Among other benefits, cyber insurance policies provide access to data breach consultants and other experts to assist firms that suffer data breaches. These policies cover expenses for forensic investigation and public relations assistance, notification costs, credit monitoring, and consumer education and assistance costs arising out of data breaches. Many policies also cover the cost of retaining counsel to evaluate a firm's potential obligations if a breach occurs.

1 For a discussion of cyber risk insurance, see Christopher Fill, *Cyber Risk and Insurance for Law Firms*, QUALITY ASSUR. REV., Winter 2012, at 10.

Contacts

For more information on our Loss Prevention Services, please contact:

Douglas R. Richmond
+1.312.381.7121
doug.richmond@aon.com

Henry S. Bryans
+1.610.995.0488
henry.bryans@aon.com

Matthew K. Corbin
+1.816.698.4660
matthew.corbin@aon.com

Jane Hunter
+44 (0)20.7086.2160
jane.hunter@aon.co.uk

Mark J. Peterson
+1.402.203.5396
mark.peterson1@aon.com

For information about cyber risk insurance, please contact:

Mark Greenwood
+1.212.441.1776
mark.greenwood@aon.com

Christopher Fill
+1.312.381.3825
christopher.fill@aon.com

Tom Ricketts
+1.212.441.1744
tom.ricketts@aon.com

About Professional Services

Aon Risk Solutions' Professional Services practice is Aon's unified global team of insurance brokers, reinsurance brokers and insurance consultants/advisors dedicated solely to serving professional service firms; including Accountants, Architects, Engineers, Surveyors and other Design and Project Professionals, Consultants, Lawyers, Solicitors and Notaries. Professional Services offers over 75 years of unique and extensive knowledge on issues relevant to professional service firms by providing strategic advice and innovative solutions tailored to meet the specific needs of individual clients. The market access and expertise, value added services and integrated global platform enhance the compelling value proposition. Through a dedicated team of more than 200 practitioners globally, Professional Services practice represents more large professional service firms than any other broker in the world. Please visit www.aon.com/professional services for more information.

About Aon

Aon plc (NYSE:AON) is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 66,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative and effective risk and people solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world's best broker, best insurance intermediary, reinsurance intermediary, captives manager and best employee benefits consulting firm by multiple industry sources. Visit www.aon.com for more information on Aon and www.aon.com/manchesterunited to learn about Aon's global partnership and shirt sponsorship with Manchester United.

www.aon.com

Risk. Reinsurance. Human Resources.

AON
Empower Results®

Richmond Journal of Law & Technology Volume XXI, Issue 3

BEYOND TECHNOPHOBIA: LAWYERS' ETHICAL AND LEGAL OBLIGATIONS TO MONITOR EVOLVING TECHNOLOGY AND SECURITY RISKS

Timothy J. Toohey*

Cite as: Timothy J. Toohey, *Beyond Technophobia: Lawyers' Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks*, 21 RICH. J.L. & TECH. 9 (2015), http://jolt.richmond.edu/v21i3/article9.pdf.

I. INTRODUCTION

[1] Lawyers and technology have an uneasy relationship. Although some lawyers are early adapters, others take pride in ignoring technology because they believe it is alien to the practice of law. As Jody R. Westby observed, lawyers confronted with technology and security issues tend to have their "eyes glaze over" and "want to call in their 'IT guy' and go back to work."[1] But this technophobic attitude may no longer just be harmless conservatism. In the world of growing security risks, ignorance of technology may lead to violations of lawyers' fundamental ethical duties of competence and confidentiality.

[2] As with other businesses, lawyers are part of a constantly evolving and interconnected data ecosystem. The pervasiveness of electronic data in all aspects of commercial and personal life and its easy transmission through the Internet have not only fundamentally altered the manner in which lawyers interact with clients and with one another, but potentially expose confidential and proprietary information to rapid and unauthorized dissemination. As vast amounts of data are created and stored,

* Partner, Head of Cyber, Privacy and Data Security Practice at Morris Polich & Purdy, Los Angeles, California; Certified Information Privacy Professional United States and European Union (CIPP/US/E); Certified Information Privacy Manager (CIPM).

[1] Jody R. Westby, *Cybersecurity & Law Firms: A Business Risk*, 39 L. PRACTICE MAG. 4, 46 (July–Aug. 2013), *available at* http://www.lawpracticemagazine.com/lawpracticemagazine/july_august_2013#pg1,

confidential data—including attorney-client communications—can be readily transferred or accessed by unauthorized parties. With rapidly changing technology and threat vectors, lawyers are increasingly challenged in maintaining the security of their information and that of their clients.

[3] Rapid technological change has been a constant for the practice of law for at least a generation. E-mail, which in the early 1990s was not widely used in the profession, is now the main form of communication within law firms, as well as with counsel and clients outside the firm. Despite the growth of text messaging, e-mail continues to expand as a means of business communication. In 2011 there were on average 105 e-mails sent or received by corporate users per day, and it is predicted that this will increase to 125 e-mails per day by 2015.[2] While in 2011 there were over 3.1 billion e-mail accounts (of which 788 million were corporate), it is predicted that in 2015 there will be four billion accounts (of which over one billion would be corporate).[3]

[4] The use of the Internet, which impacts almost every aspect of the practice of law, has also grown substantially in the last twenty years. In 1995 there were sixteen million users worldwide, in 2005 over a billion, and as of June 2014 it is estimated that there are over three billion users.[4] In the past, lawyers used their own in-house computing resources. But now, facilitated by the Internet, lawyers frequently use remote provisioning of computing and storage services known as "cloud computing." It is predicted the future will show a 44% annual growth in

archived at http://perma.cc/VBR2-2RAM.

[2] *See* SARA RADICATI & QUOC HOANG, EMAIL STATISTICS REPORT, 2011-2015 3 (2011), *available at* http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf, *archived at* http://perma.cc/2SLA-4CD8.

[3] *See id.* at 2–3.

[4] *See Internet Growth Statistics*, INTERNET WORLD STATS, http://www.internetworldstats.com/emarketing.htm (last updated Dec. 1, 2014 *archived at* http://perma.cc/27N9-68YE.

public cloud workloads, in comparison to an 8.9% annual growth for computing services located in the premises of businesses.[5] In 2014 it was estimated that there was one exabatye (i.e., 10^{18} bytes of data) stored in the cloud, and CISCO predicts data center traffic will triple by 2017.[6]

[5] This article argues that because of the evolving security risks brought by the changes wrought by e-mail, the Internet, and cloud computing, lawyers must reassess their ethical duties of competence and confidentiality. Although lawyers may have been comforted by ethical opinions finding the use of e-mail or cloud computing appropriate in the past, they can no longer rely on those opinions given dramatically altered security risks.

[6] This article also argues that lawyers must develop a greater awareness of the risks posed by the technology than they have had in the past because—like their clients—they are subject to rapidly escalating security threats. Whether they are aware of it or not, lawyers and law firms are increasingly the target of sophisticated hackers who deliberately seek out the confidential information they store on behalf of clients.[7] Although lawyers should not (and, indeed, cannot) abandon e-mail and cloud computing, they must shoulder greater responsibility in protecting data against evolving security risks. Lawyers must take concrete steps to protect data which they store for themselves and their clients, including developing risk management and incident response programs to prepare for cyberattacks and the consequences of such attacks. As with their corporate counterparts, security and privacy are no longer a matter for

[5] *See* Jack Woods, *20 Cloud Computing Statistics Every CIO Should Know*, SILICONANGLE (Jan. 27, 2014), http://siliconangle.com/blog/2014/01/27/20-cloud-computing-statistics-tc0114/, *archived at* http://perma.cc/GVQ2-MHRR.

[6] *See id.*

[7] *See, e.g.*, Andrew Conte, *Unprepared Law Firms Vulnerable to Hackers*, TRIBLIVE (Sept. 13, 2014, 10:40 PM), http://triblive.com/news/allegheny/6721544-74/law-firms-information#axzz3S2IsKaPf, *archived at* http://perma.cc/9DUR-HQXF (stating that computer hackers are targeting top international law firms to steal intellectual property data and trade secrets).

specialists, but for all who deal with private, proprietary, and confidential data—including lawyers.[8]

II. LAWYERS AND TECHNOPHOBIA

[7] Although it is unlikely there will ever be a comprehensive study of the subject, a portion of the legal profession—if not outright Luddites—are uncomfortable with technology and consider an understanding of its workings to be unnecessary—if not inimical—to the practice of law.[9] In a 1963 article on "Lawyers and Machines," Colin Tapper observed that "[l]awyers are traditionally conservative" and resistant to change, including when it comes to adopting machines for their work.[10] Tapper presciently suggested what we would now call computerized databases could be useful in the practice of law, but feared that lawyers may be slow to accept such tools.[11] Although Tapper believed technology had brought

[8] *See, e.g.*, Richard Blackwell, *C-Suite Survey: Cybersecurity Becomes A Top Priority After Data Breaches*, BUS. NEWS NETWORK (Oct. 20, 2014, 10:09 AM), http://www.bnn.ca/News/2014/10/20/C-Suite-Survey-Cybersecurity-becomes-a-top-priority-after-data-breaches.aspx, *archived at* http://perma.cc/Y4X7-WPHP; *see also* JODY R. WESTBY, GOVERNANCE OF ENTERPRISE SECURITY: CYLAB 2012 REPORT: HOW BOARDS & SENIOR EXECUTIVES ARE MANAGING CYBER RISKS 5–6 (2012), *available at* http://www.hsgac.senate.gov/imo/media/doc/CYBER%20Carneigie%20Mellon%20report.pdf, *archived at* http://perma.cc/3CXW-4QKM (reporting that boards of directors are still "not actively addressing cyber risk management").

[9] *See* Maureen O'Neill, *Lawyers Must Conquer Technophobia to Provide Competent Counsel*, DISCOVER READY (May 24, 2012), http://discoverready.com/blog/lawyers-must-conquer-technophobia-to-provide-competent-counsel/, *archived at* http://perma.cc/92TG-NLT5; *see also* Mitch Kowalski, *New Legal Tech Audit Will Scare Lawyers into Embracing Technology*, LEGAL POST, (Aug. 29, 2014, 2:12 PM), http://business.financialpost.com/2014/08/29/new-legal-tech-audit-will-scare-lawyers-into-embracing-technology/, *archived at* http://perma.cc/U46T-3V35 ("Lawyers have traditionally revelled in their technophobia—much to their client's chagrin."); Kenneth N. Rashbaum et al., *Cybersecurity: Business Imperative for Law Firms*, N.Y. L.J. (Dec. 10, 2014), http://www.newyorklawjournal.com/id=1202678493487/Cybersecurity-Business-Imperative-for-Law-Firms, *archived at* http://perma.cc/2GVN-4XFT (referencing the "reputed technophobia of many lawyers").

[10] *See* Colin Tapper, *Lawyers and Machines,* 26 MOD. L. REV. 121, 122 (1963).

improvements, including the use of the Dictaphone, he noted that as late as the 1960s the Chancery Division of the English law courts resisted using "typewriters, the postal service and telephones."[12]

[8] Like their English counterparts, some U.S. lawyers have historically been resistant to adopting new technology. When future U.S. Secretary of State John Foster Dulles joined Sullivan & Cromwell in 1911, telephones and stenographers were not widely accepted and some "partners felt that the only dignified way of communication between members of the legal profession was for them to write each other in Spencerian script,[13] and to have the message thus expressed [sic] delivered by hand."[14] Clarence Seward, the managing partner of what would become Cravath, Swaine & Moore "'sought in vain to save the office from the machine [including elevators and typewriters], which was destroying the simplicity of American life.'"[15]

[9] Notwithstanding initial resistance, the U.S. legal profession eventually embraced elevators, typewriters and Dictaphones—as it would later adopt the Telex, copiers, fax machines, personal computers,

[11] *See id.*

[12] *Id.* at 122 n. 1.

[13] Spencerian script was a "script style that was used in the United States from approximately 1850 to 1925 and was considered the American *de facto* standard writing style for business correspondence prior to the widespread adoption of the typewriter." *Spencerian Script*, WIKIPEDIA, https://en.wikipedia.org/wiki/Spencerian_script, *archived at* https://perma.cc/2FHM (last modified June 24, 2014, 12:59 PM).

[14] Catherine J. Lanctot, *Attorney-Client Relationships in Cyberspace: The Peril and the Promise*, 49 DUKE L. J. 147, 164 (1999) (quoting John Foster Dulles, *Foreword* to ARTHUR H. DEAN, WILLIAM NELSON CROMWELL 1854–1984, at iii (1957)).

[15] *Id.* at 165 (quoting ROBERT T. SWAINE, THE CRAVATH FIRM AND ITS PREDECESSORS, 1819-1947, at 448 (1946)). Lanctot writes that "[i]n a story so telling that it can only be apocryphal, one colleague described the time that Seward refused to take an elevator up four flights to a hearing in federal court and insisted instead on walking. When he finally arrived at the courtroom, Seward was reportedly so out of breath that the argument had to be cancelled and the case submitted on the briefs." *Id.*

electronic mail, mobile phones, and electronic research databases. [16] Today's lawyers are unlikely to reject technology outright, because that would render them virtually incapable of communicating with one another and their clients and practicing law. Nonetheless, a substantial number of lawyers exhibit a sometimes studied indifference to technology, believing it to be either irrelevant to the practice of law or the purview of non-lawyers—including the IT department.[17]

III. SECURITY RISKS AND THE PRACTICE OF LAW

[10] Given their unsettled relationship with technology, lawyers have been slow to recognize that hackers have lawyers in their sights as a potentially easy target. Lawyers who "have a hard enough time just figuring out how to work their BlackBerry or iPhone" [18] may have difficulty understanding that they are "basically the same as any other company when it comes to countering cyberattacks and protecting their confidential and proprietary data."[19] But, in fact, lawyers have been warned for at least the last five years that they are susceptible to cyberattacks because of the substantial amounts of data they safeguard for themselves and their clients.[20]

---

[16] *See* Robert Ambrogi, *A Chronology of Legal Technology, 1842–1995*, L. SITES (Feb. 14, 2010), http://www.lawsitesblog.com/2010/02/chronology-of-legal-technology-1842.html, *archived at* http://perma.cc/NU4C-NFVX; *see also* Nicole Black, *10 Technologies That Changed the Practice of Law*, MYCASE (July 29, 2014), http://www.mycase.com/blog/2014/07/10-technologies-changed-practice-law/, *archived at* http://perma.cc/SRT5-A6QS.

[17] *See* Westby, *supra* note 1, at 46–47.

[18] Jennifer Smith, *Lawyers Get Vigilant on Cybersecurity*, WALL ST. J., June 26, 2012, *available at* http://www.wsj.com/articles/SB10001424052702304586045774867611017267 48, *archived at* http://perma.cc/2V83-AP92.

[19] Westby, *supra* note 1, at 46.

[20] *See* Michael Cooney, *FBI Warns of Spear Phishing Attacks on Lawyers, PR Firms*, NETWORKWORLD (Nov. 18, 2009, 3:20 PM),

[11] As cyberattacks have grown in number, so has the exposure of the legal profession to such attacks. In the last two years, cyberattacks on U.S. enterprises have been constantly in the news. 2014 has been proclaimed the "year of the data breach" because of the well-publicized attacks on Target, Home Depot, Sony Pictures Entertainment (SPE), and numerous other businesses.[21] Even before the SPE breach in November 2014, Forrester Research predicted that "[a]t least 60% of brands will discover a breach of sensitive data in 2015, with the actual number of breached entities being as high as 80% or more . . . ."[22]

[12] The Verizon 2014 Data Breach Investigations Report, which is based on reported events from 2013, referenced 63,437 reported security incidents and 1,367 breaches in almost every economic sector.[23] Of interest to lawyers is the fact that the Verizon Report found that attacks on "professionals" have grown significantly in recent years with only the public sector, finance and retail having more security incidents than professionals in 2013.[24]

[13] The primary attack vectors for professionals include "denial of service" (DoS) attacks and cyber espionage.[25] DoS attacks typically

http://www.networkworld.com/article/2232563/security/fbi-warns-of-spear-phishing-attacks-on-lawyers--pr-firms.html, *archived at* http://perma.cc/HDV5-4LXZ.

[21] *See* Tom Huddleston, Jr., *The Sony Hack Should Make Cyber Security a Hot Boardroom Topic*, FORTUNE (Dec. 23, 2014, 1:55 PM), http://fortune.com/2014/12/23/sony-hack-security-boardroom/, *archived at* http://perma.cc/R62B-NEUF.

[22] *60% of Brands Will Discover a Breach of Sensitive Data in 2015*, FORRESTER (Nov. 12, 2014), https://www.forrester.com/60+Of+Brands+Will+Discover+A+Breach+Of+Sensitive+Data+In+2015/-/E-PRE7425, *archived at* https://perma.cc/C9S6-A88J.

[23] *See* VERIZON, 2014 DATA BREACH INVESTIGATIONS REPORT 2 (2014), *available at* http://www.verizonenterprise.com/DBIR/2014/, *archived at* http://perma.cc/B2KR-4LT9.

[24] *See id.* at 15.

compromise the availability of networks and systems through network and computer applications.[26] DoS attacks may be launched by either individuals or entities, including foreign governments, competitors and disgruntled employees. The aim of a DoS attack is to slow or shut down legitimate traffic to the victim's website.[27] Almost any type of business may be subject to a DoS attack and such attacks may be launched for a wide variety of reasons, including shutting down a controversial project, preventing access to financial or other key services, gaining publicity for a cause, or benefiting a foreign government or competitor.[28]

[14] Another major source of attacks against professionals is cyber espionage, in which state-affiliated actors, particularly from Asia and Eastern Europe, target enterprises to obtain information of competitive or strategic value.[29] Cyber espionage attacks are often conducted through malware implanted on computer systems by way of a social engineering attack, such as "spear-phishing" e-mails.[30] In a targeted attack, the user

[25] *See id.*

[26] *See id.* at 43–45.

[27] *See* TIMOTHY J. TOOHEY, PRIVACY AND DATA SECURITY TRENDS AND DESIGN PROFESSIONALS 1–2 (Morris Polich & Purdy 2014) [hereinafter PRIVACY AND DATA SECURITY TRENDS AND DESIGN PROFESSIONALS], *available at* http://www.mpplaw.com/files/Publication/c76f880b-a26b-4d33-91eb-e629890feeca/Presentation/PublicationAttachment/de6cbf28-77b2-4389-ad01-e6a0f3a741eb/DR-Privacy-and-Data-Security-Trends-and-Design-Professionals-TJT-June-2014.pdf, *archived at* http://perma.cc/WKC2-JNDX.

[28] *See id.* at 2; *see also* Bob Tarzey, *Why Would They DoS Us?*, COMPUTERWEEKLY (Feb. 10, 2014, 7:54 AM), http://www.computerweekly.com/cgi-bin/mt-search.cgi?blog_id=119&tag=Denial-of-service%20attack&limit=20, *archived at* http://perma.cc/XYS6-KARF.

[29] *See, e.g.*, PRIVACY AND DATA SECURITY TRENDS AND DESIGN PROFESSIONALS, *supra* note 27, at 2.

[30] *See* Pieter Danhieux, *Email Phishing Attacks*, OUCH! (Sans Institute), Feb. 2013, at 1, *available at* http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_en.pdf, *archived at* http://perma.cc/M3WW-MCVD.

typically receives a seemingly bona fide e-mail from what appears to be a colleague which in fact comes from a hostile party.[31] When the recipient clicks on an executable file in the e-mail, malware is launched that is implanted into the recipient's computer system.[32]

[15] Although some of the details are unclear, the massive breach against SPE's computer systems in November and December 2014 is in key respects akin to a cyber espionage attack. Using malware with the capability to, among other things, access files stored on a computer system, the hackers mounted an attack on SPE that created backdoor access to the system, destroyed and "clean[ed]" computer systems, and paralyzed the company's computer systems for weeks.[33] The attack, which the U.S. attributes to North Korea, arose in conjunction with the James Franco and Seth Rogen film *The Interview* which featured a fictional plot to assassinate North Korean leader Kim Jong Un.[34] The attack rendered SPE's computer system inaccessible, and significant amounts of sensitive and proprietary data were exfiltrated from its system.[35] The attack also resulted in the release and public distribution of

[31] *See id.*

[32] *See id.* at 1–2.

[33] *See, e.g.*, Brian Krebs, *Sony Breach May Have Exposed Employee Healthcare, Salary Data*, KREBS ON SECURITY (Dec. 2, 2014, 11:21 AM), http://krebsonsecurity.com/2014/12/sony-breach-may-have-exposed-employee-healthcare-salary-data/, *archived at* http://perma.cc/3TNS-RC67; *see also Alert (TA14-353A): Targeted Destructive Malware*, U.S. COMPUTER EMERGENCY READINESS TEAM (Dec. 19, 2014), https://www.us-cert.gov/ncas/alerts/TA14-353A, *archived at* https://perma.cc/KB5E-29AR (analyzing malware used to attack SPE).

[34] *See, e.g* , David E. Sanger & Michael S. Schmidt, *More Sanctions on North Korea After Sony Case*, N.Y. TIMES, Jan. 3, 2015, at A1, *available at* http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html, *archived at* http://perma.cc/4QVA-NPKE.

[35] *See* Ben Fritz and Danny Yadron, *Sony Hack Exposed Personal Data of Hollywood Stars*, WALL ST. J., Dec. 5, 2014, *available at* http://www.wsj.com/articles/sony-pictures-hack-reveals-more-data-than-previously-believed-1417734425 *archived at* http://perma.cc/6UHK-RQBY.

sensitive attorney-client communications, including materials relating to labor matters handled by a prominent U.S. law firm, e-mails from SPE executives, and 47,000 social security numbers of current and former SPE employees, including actors and directors.[36]

[16] Social engineering attacks are not limited to those engaging in cyber espionage. For example, in the 2013 Target hack, a social engineering attack against one of Target's vendors launched malware that allowed cyber criminals in Eastern Europe to obtain credit card information from Target's customers at the point of sale (POS).[37] The malware lurked on Target's system for weeks and automatically sent credit card information for 70–110 million individuals to the hackers.[38]

[17] Cyber espionage attacks are particularly difficult to detect. The Verizon 2013 Report found that 62% of the attacks took months to discover and 5% of attacks took years to detect.[39] Aside from the SPE attack, which appears to have been motivated less by economic than political motives, attacks are typically launched by foreign nation states to obtain information to allow them to gain advantage for a particular project. For example, in May 2014 the U.S. Department of Justice announced it had charged Chinese military hackers with cyber espionage aimed at

[36] *See id.*; *see also* Debra Cassens Weiss, *Sony Pictures Hires David Boies, Who Warns Media to Destroy Documents Leaked by Hackers*, ABA Journal (Dec. 15, 2014 11:38 AM), http://www.abajournal.com/news/article/sony_pictures_hires_david_boies_who_warns_media_to_destroy_hacked_documents, *archived at* http://perma.cc/33FK-8XBZ.

[37] *See* Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KREBS ON SECURITY (Feb. 5, 2014, 1:52 PM), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/, *archived at* http://perma.cc/F2JR-9ZYE.

[38] *See* Elizabeth A. Harris and Nicole Perlroth, *For Target, The Breach Numbers Grow*, N.Y. TIMES, Jan. 11, 2014, at B1, *available at* http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html?_r=0, *archived at* http://perma.cc/GH83-UUQD.

[39] *See* VERIZON, *supra* note 23, at 41.

obtaining "confidential and proprietary technical and design specifications" from several U.S. companies, including Westinghouse, to advantage Chinese state-owned enterprises.[40]

[18] Law firms are far from immune to security attacks, including DoS and cyber espionage attacks.[41] In its August 2014 cybersecurity resolution, the ABA found that "[t]he threat of cyber attacks against law firms is growing" and that "[l]awyers and law firms are facing unprecedented challenges from the widespread use of electronic records and mobile devices."[42] Lawyers and law firms are targets because "[t]hey collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-[D]iscovery."[43] As a former FBI agent has observed, law firms are vulnerable to attack because they "'have incredibly valuable and sensitive information, and the Internet just provides a whole other methodology through which the information can be accessed and pilfered.'"[44] Lawyers may also be targets

[40] *See* Press Release, U.S. Dept. of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), *available at* http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor, *archived at* http://perma.cc/XYJ8-DQJX

[41] *See* Rashbaum et al., *supra* note 9.

[42] JUDITH MILLER AND HARVEY RISHIKOF, ABA, CYBERSECURITY LEGAL TASK FORCE SECTION OF SCIENCE & TECH. LAW REPORT TO THE HOUSE OF DELEGATES 4 (2014), *available at* http://www.americanbar.org/content/dam/aba/events/law_national_security/2014annualmeeting/ABA%20-%20Cyber%20Resolution%20109%20Final.authcheckdam.pdf, *archived at* http://perma.cc/ACE4-GAKC; *see also American Bar Association House of Delegates Adopts Resolutions on Cybersecurity, Domestic Violence*, ABA (Aug. 12, 2014), http://www.americanbar.org/news/abanews/aba-news-archives/2014/08/american_bar_associa.html, *archived at* http://perma.cc/G9AL-8T9N.

[43] MILLER AND RISHIKOF, *supra* note 42, at 4.

[44] Smith, *supra* note 18 (quoting Shawn Henry, a "FBI veteran former executive assistant director of the agency's criminal, cyber, response and services branch.").

of attacks because "it is generally easier for a hacker to break into a law firm's network to steal client data than it is to hack into the clients' networks to steal the data."[45]

[19] Few law firm hacks have been publicized, most likely because the firms are reluctant publicly to expose their vulnerability and may not legally be required to inform the public of hacks.[46] However, it has been reported that an unnamed "major New York law firm" was attacked in 2012 by Chinese hackers seeking information about a business deal.[47] When this hack was announced, the FBI "convened a meeting with the top 200 New York City law firms to address the rising number of cyberattacks on law firms."[48] The FBI reportedly warned lawyers at the meeting "that they were easy prey for hackers trying to obtain their clients' valuable data."[49] Law firms were an "easy target," according to the FBI, because "partners insist on mobility—including the ability to review case documents at home on the weekend or while travelling—which means highly sensitive documents are routinely transferred by e-mail, leaving them vulnerable to attack."[50] The FBI informed lawyers at the meeting that it had "'seen specific documents from law firms on specific deals being exfiltrated from cyberattacks.'"[51]

[45] Lynn Watson, *At the Crossroads of Lawyering and Technology: Ethics*, PRACTICE INNOVATIONS, July 2012, at 17, 18, *available at* http://info.legalsolutions.thomsonreuters.com/signup/newsletters/practice-innovations/2013-jan/Jan13_PracticeInnovations.pdf, *archived at* http://perma.cc/H67Z-NE5F.

[46] *See* Conte, *supra* note 7.

[47] *See* Mike Mintz, *Cyberattacks on Law Firms-A Growing Threat*, MARTINDALE.COM BLOG (Mar. 19, 2012), http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat, *archived at* http://perma.cc/H67Z-NE5F.

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Smith, *supra* note 18 (quoting Mary Gallian of the FBI).

[20] Documents held by law firms are of undoubted interest to hackers. In some instances, documents originating from law firms have been exposed when hackers attack a firm's clients. For example, in the recent SPE attack, documents originating from a prominent labor and employment firm were published on the Internet, including documents that apparently contained details regarding termination of employees.[52] In another attack said to have been launched by Wikileaks in retaliation for the claim of a security firm that boasted it could identify individuals belonging to that hacktivist organization, documents were put on line from a national law firm relating to representation of clients such as Bank of America and the U.S. Chamber of Commerce.[53]

IV. LAWYERS' LEGAL AND ETHICAL OBLIGATIONS TO SECURE DATA

[21] In common with other enterprises, lawyers are legally required to secure personal data they hold on behalf of others and for themselves. In addition to being obligated to secure personal data, lawyers are also ethically bound as professionals to maintain the confidentiality of client documents and communications, which is a much broader category than "personal" information.

A. Lawyers' Legal Obligations to Secure Data

[22] Federal and state laws impose legal obligations on law firms, like other enterprises, to implement "reasonable" security measures to protect data that they store on behalf of themselves and others. These laws also require enterprises to report any breaches in the security of personal data.

[23] For example, Cal. Civ. Code § 1798.81 requires businesses to take

[52] *See* Krebs, *supra* note 33 (showing screen shot of file tree including references to law firm and employee data).

[53] *See* Brian Baxter, *Hunton & Williams Linked to Hacked E-Mail Affair*, AMLAW DAILY (Feb. 15, 2011, 11:11 AM), http://amlawdaily.typepad.com/amlawdaily/2011/02/hunton-wikileaks.html, *archived at* http://perma.cc/7RKU-V6LG.

"reasonable steps to dispose, or arrange for the destruction of customer records within its custody or control containing personal information."[54] Cal. Civ. Code § 1798.81.5 also requires businesses that "own" or "license" personal information about a California resident to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification, or disclosure."[55] As of January 1, 2015, California will also require businesses that "maintain" information on behalf of others to implement such security measures, for "information that a business maintains but does not own or license."[56]

[24] California and forty-seven other states require persons and businesses, including lawyers, to notify residents regarding breaches of unencrypted personal information.[57] In California, which has led the way in such data breach notification laws, "personal information" includes (1) an individual's first name or first initial and last name in combination with a social security number, a driver's license or identification card number, an account number, credit or debit card number in combination with a

[54] CAL. CIV. CODE § 1798.81 (Deering 2005). The statute further requires that records are to be shredded or erased or that the personal information in the records should be made "unreadable or undecipherable through any means."

[55] *Id.* at § 1798.81.5.

[56] *See* A.B. 1710, 2013–2014 Gen. Assemb., Reg. Sess. (Cal. 2014)., *available at* http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710, *archived at* http://perma.cc/HL69-CJDV; *see also* Timothy J. Toohey, *California Modifies Its Data Breach Notification Requirements Again*, MORRIS POLICH & PURDY (Oct. 3, 2014) [hereinafter *California Modifies Its Data Breach Notification Requirements Again*], http://privacydatasecurity.com/CA-Modifies-Data-Breach-Notification-AB-1710-TJT-10'3'14.pdf, *archived at* http://perma.cc/SK3S-8LGD.

[57] *See* CAL. CIV. CODE § 1798.82 (Deering 2005). A list of the data breach laws is maintained by the National Conference of State Legislatures. *See Security Breach Notification Laws*, NAT'L CONFERENCE OF STATE LEGISLATURES (Jan. 12, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx, *archived at* http://perma.cc/V9JZ-UYJZ (maintaining a list of data breach laws).

required security code, access code or password, medical information, or health insurance information or (2) a user name and e-mail address in combination with a password or security question and answer that would permit access to an online account.[58] Moreover, if the personal information that is breached is not owned by the person or business that was breached, they must "notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[59] Failures of businesses, including law firms, to maintain appropriate security or to comply with data breach notification laws, may subject them to fines and/or lawsuits for damages.[60]

[25] Federal authorities may also penalize businesses that do not maintain appropriate security measures. For example, the Federal Trade Commission (FTC) has broad authority under Section 5 of the FTC Act[61] to bring actions against enterprises that do not maintain "reasonable and appropriate data security for consumers' sensitive personal information."[62]

[58] *See* CAL. CIV. CODE § 1798.82(e).

[59] *Id.* at § 1798.82(b).

[60] *See id.* at § 1798.84. For example, the California Attorney General brought an action against Kaiser Foundation Health Plan alleging that the disclosure of a breach was unreasonably delayed when personal data was found in a hard drive being sold at a thrift store. *See* Ronald W. Breaux, Emily Westridge Black, and Timothy Newman, *California AG Cracks Down on Timing of Data Breach Disclosures*, HAYNES BOONE (Feb. 5, 2014), http://www.haynesboone.com/california-ag-cracks-down-on-timing-of-data-breach-disclosures-02-04-2014/, *archived at* http://perma.cc/M8CK-KCWA. Kaiser settled the matter for $150,000.00. *Id.*

[61] *See* 15 U.S.C. § 45(a)(1) & (2) (2012). The Act declares unlawful "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce . . . ." *Id.* The FTC's enforcement generally proceeds under either the "unfairness" prong which focuses on consumer injury or the "deception" prong which focuses on "[a] representation, omission, or practice [which] misleads or is likely to mislead the consumer." *See* TIMOTHY J. TOOHEY, UNDERSTANDING PRIVACY AND DATA PROTECTION: WHAT YOU NEED TO KNOW 107–08 (2014) [hereinafter UNDERSTANDING PRIVACY AND DATA PROTECTION].

The FTC may take administrative actions against entities that do not maintain reasonable security measures, which typically result in consent decrees requiring businesses to put in place a comprehensive security program and undertake periodic audits or reviews by a certified third party for up to 20 years.[63]

[26] Law firms, like other enterprises, are also subject to federal laws that require implementation of security measures. For example, law firms may be considered "business associates" under the Health Information Privacy Protection Act (HIPAA)[64] because they perform functions for health care clients, such as reviewing documents that contain health care information.[65] As HIPAA business associates, law firms must follow the

[62] Fed. Trade Comm'n v. Wyndham Worldwide Corp., No. 13-1887 (ES), 2014 U.S. Dist. LEXIS 84913, at *1 (D.N.J. June 23, 2014).

[63] *See* Press Release, Fed. Trade Comm'n, Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information (Jan. 31, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it, *archived at* http://perma.cc/K6ST-U33C. The settlement with the company in question (GMR Transcription) was the 50th data security case settled by the FTC. *Id.*

[64] *See* Matthew H. Meade, *Lawyers and Data Security: Understanding a Lawyer's Ethical and Legal Obligations That Arise from Handling Personal Information Provided by Clients*, 28 COMPUTER & INTERNET LAWYER 1, 7 (Oct. 2011), *available at* http://www.bipc.com/files/Publication/ae615839-5e8f-4ce6-99af-a6aed9bc6a69/Preview/PublicationAttachment/2ea3d9ea-61bc-4324-8cee-5df5f01e07dd/CIL_1011_Meade.pdf, *archived at* http://perma.cc/2WT5-36J8.

[65] According to the United States Department of Health and Human Services, a "business associate" is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity." U.S. DEP'T OF HEALTH AND HUMAN SERV., BUSINESS ASSOCIATES 1 (2009), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.pdf, *archived at* http://perma.cc/8HWY-QNGR. The rules relating to business associates are set forth in 45 C.F.R. § 164.502(e) (2014), 45 C.F.R. § 164.504(e) (2014), 45 C.F.R. §164.532(d) (2014) and 45 C.F.R. §164.532(e) (2014). A "covered entity" is a provider of health care services and "protected health information" (sometimes referred to as PHI) is all "individually identifiable health information" held or sent by a "covered entity or its

HIPAA Security Rule[66] requiring them to put in place safeguards to secure electronic protected health information. Although the HIPAA Security Rule does not require specific security measures, it recommends implementing procedures to insure the confidentiality, integrity, and availability of electronic protected health information to protect against reasonably anticipated threats and impermissible uses or disclosures, and to ensure compliance by an entity's employees.[67] If a law firm is a HIPAA business associate, it must also report breaches of protected health information to the United States Department of Health and Human Services and may be subject to fines for such breaches.[68]

B. Lawyers' Ethical Obligations to Maintain Client Confidences

[27] In addition to being subject to state and federal laws affecting other enterprises, lawyers also have independent ethical duties requiring them to be aware of the risks of technology and to implement measures to protect against unauthorized disclosure of confidential information.

[28] The ABA Model Rules of Professional Conduct ("ABA Model Rules"), which are followed by most states, establish a competence requirement in Rule 1.1 that "[a] lawyer shall provide competent

business associate, in any form or media, whether electronic, on paper, or oral." *See Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T OF HEALTH AND HUMAN SERV., *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html, *archived at* http://perma.cc/483U-CWKY (last visited Jan. 20, 2014).

[66] *See* 45 C.F.R. § 164.502(a)(1) (2013).

[67] *See* UNDERSTANDING PRIVACY AND DATA PROTECTION, *supra* note 61, at 37–38.

[68] *See California Modifies Its Data Breach Notification Requirements Again*, *supra* note 56, at 37–39.

representation to a client."[69] The ABA Model Rules further state "[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[70] Since 2012, comment 8 to Rule 1.1 has provided that "[t]o 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."[71]

[29] Rule 1.6 of the ABA Model Rules establishes the duty for lawyers to maintain the confidentiality of information and requires that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent . . . ."[72] Rule 1.6 further provides 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."[73]

[30] Since 2012, comment 18 to ABA Model Rule 1.6(c) has "require[d] 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."[74]

[69] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2014).

[70] *Id.* States have adopted these changes, including Pennsylvania. *See* Shannon Brown, *Pennsylvania's New, Technology-related Ethics Rule Changes for Lawyers*, SHANNON BROWN LAW (Mar. 21, 2014), http://www.shannonbrownlaw.com/archives/2109, *archived at* http://perma.cc/Z5V8-2CEK.

[71] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2014) (emphasis added).

[72] *Id.* at R. 1.6(a).

[73] *Id.* at R. 1.6(c).

[74] *Id.* at R. 1.6 cmt. 18.

[31] If the lawyer has "made reasonable efforts to prevent the access of disclosure" the Rule is not violated.[75] Comment 18 further states that

> Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, 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 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.[76]

[32] In Formal Opinion 2010-179, the California Standing Committee on Professional Responsibility and Conduct addressed an issue similar to that addressed in the 2012 comments to the ABA Model Rules. Opinion 2010-179 discussed the issue of whether an attorney violates the duties of confidentiality and competence owed to a client "by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties."[77] The specific

[75] *Id.*

[76] *Id.*

[77] State Bar of California Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 at 1 (discussing whether an attorney violates duties of confidentiality and

context for the opinion was whether an attorney using a laptop to conduct legal research and e-mail a client through a public wireless Internet connection and through the attorney's personal wireless system violated any ethical rules.[78]

[33] Opinion 2010-179 concluded that the use of a public wireless connection without using precautions, such as encryption or a personal firewall, risked violating the attorney's duties of confidentiality and competence because of the "lack of security features provided in most public wireless access locations."[79] In contrast, the opinion found that the use of the attorney's personal wireless system would not violate the attorney's duties if the system were "configured with appropriate security features."[80]

[34] Opinion 2010-179 adopted a flexible analytic approach to technology, recognizing that technology is "ever-evolving" and is now integrated in "virtually every aspect of our daily lives."[81] The opinion further recognized that "guidance to attorneys in this area has not kept pace with technology" and "[m]any attorneys, as with a large contingent of the general public, do not possess much, if any, technological savvy."[82] Although the opinion found it was unnecessary for attorneys to develop a mastery of the security features and deficiencies of each technology available, *the duties of confidentiality and competence that attorneys owe*

competence when using technology to transmit or store confidential client information that may be susceptible to unauthorized access by third parties), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836, *archived at* http://perma.cc/Z2NX-ZWF5.

[78] *See id.*

[79] *Id.* at 7.

[80] *See id.* (noting that features such as firewalls, antivirus and anti-spam software, secure username and password combinations, and file permissions as "appropriate.").

[81] *Id.* at 1.

[82] *Id.* at 1, 5.

to their clients do require a basic understanding of the electronic protections afforded by the technology they use in their practice. If the attorney lacks the necessary competence to assess the security of the technology, he or she must seek additional information or consult with someone who possesses the necessary knowledge, such as an information technology consultant.[83]

[35] Opinion 2010-179 further emphasized that attorneys must ensure that law firm personnel are "appropriately instructed regarding client confidentiality and are supervised in accordance with rule 3-110."[84] Because of "the evolving nature of technology and differences in security features that are available, the attorney *must ensure the steps are sufficient for each form of technology being used and must continue to monitor the efficacy of such steps.*"[85]

[36] California Formal Opinion 2010-179, combined with the 2012 revisions to the ABA Model Rules, place an affirmative obligation on lawyers not merely to be generally aware of the risks of technology, but to understand how risks relating to a specific technology are evolving. A technology that may have been safe when it was introduced may no longer be secure if risks have developed that undermine confidentiality protections.

[37] In addition, both the ABA Model Rules and California Formal Opinion 2010-179 place an obligation on lawyers to implement a security

[83] State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179 at 5, (emphasis added) (citing Cal. Rules Prof. Conduct, R. 3-110(C) (2013) ("If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by (1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or (2) by acquiring sufficient learning and skill before performance is required.")), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836, *archived at* http://perma.cc/F337-JV48.

[84] *Id.* at 6.

[85] *Id.* at 7 (emphasis added).

program protecting confidential data. Although the precise elements will differ for each lawyer or firm, a security program should include governance standards, "development of security strategies, plans, policies and procedures; creation of inventories of digital assets; selection of security controls; determination of technical configuration settings; performance of annual audits; and delivery of training."[86] Lawyers and law firms should also put in place a cyber response plan allowing them to detect problems, determine the cause of the problem, and resolve the problem.[87] As the ABA Cybersecurity Task Force has recommended, response plans "should be able to accommodate the full array of threats, not just data breaches."[88] Finally, as both the ABA Model Rules and the California Opinion 2010-179 recognize, law firms must put training programs in place to ensure that law firm personnel are aware of security risks and know how to help prevent cyberattacks.

V. LAWYERS' USE OF E-MAIL

[38] E-mail has become the most frequently used means of communicating within law offices and to clients, obtaining electronic alerts regarding deadlines and court filings, coordination of meetings, and accessing seemingly endless announcements of CLE seminars and communications from vendors. Because of its ubiquity, many lawyers likely believe that e-mail poses few ethical or security risks, other than the inadvertent use of "reply all."

[39] State bar associations addressing the ethics of e-mail have generally given it a green light, including lawyer use of Internet-based e-mail services, such as Gmail or Yahoo! Mail. Notwithstanding these opinions, e-mail poses significant ethical challenges for lawyers, particularly in preserving the confidentiality of communications because of security risks associated with its transmission and storage. Some web-

[86] MILLER AND RISHIKOF, *supra* note 42, at 6.

[87] *See id.* at 6.

[88] *See id.* at 9.

based e-mail providers—including Gmail—present additional challenges, because these services use e-mail content to target advertising to users and have taken the position that users have no privacy in e-mails. Finally, unencrypted e-mail entails substantial security risks, including dissemination of private communications to third parties.

A. Lawyers' Ethical Obligations and E-mail

[40] The use of unencrypted e-mail by lawyers received the blessing in 1999 of the American Bar Association Standing Committee on Ethics and Professional Responsibility ("ABA Standing Committee").[89] In Formal Opinion 99-413, the ABA Standing Committee concluded that "[a] lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[90] In reaching the conclusion, Opinion 99-413 found "[t]he same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail."[91]

[41] From today's perspective, the conclusion in Opinion 99-413 that e-mail has the "same privacy" as mail is not merely "obsolete," but misguided.[92] The fact that e-mails can be saved electronically and readily forwarded (deliberately or inadvertently) to third parties, makes them considerably less secure than mail, facsimiles, and telephone calls. To take but one current example, the embarrassing e-mails disseminated through the SPE hack that have threatened the careers of several

[89] The ABA's opinion was preceded by those of other organizations, including state bar associations. *See* Rebecca Bolin, Symposium, *Risky Mail: Concerns in Confidential Attorney-Client Email*, 81 U. CIN. L. REV. 601, 616–18 (2012).

[90] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (discussing protection of confidentiality of unencrypted e-mail).

[91] *Id.*

[92] *See* Bolin, *supra* note 89, at 603, 618.

prominent executives—including the co-chairman of the company—would not have come to light if the executives in question had confined their views to a telephone conversation or a note sent by mail.[93]

[42] In reaching its 1999 conclusion regarding e-mail privacy, the ABA Standing Committee relied on a 1998 article by David Hricik with the comforting title *E-mail and Client Confidentiality: Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*.[94] As has been noted by other commentators, Professor Hricik's reassuring conclusions regarding e-mail privacy and confidentiality depended on the then state of e-mail technology. In the mid and late 1990's, e-mails typically traveled to personal computers with limited storage space. Service providers like AOL "deleted mail off [their] servers after a few days to save on then-expensive storage."[95] In contrast, storage space today is extremely inexpensive and recipients often preserve vast numbers of sent and received e-mails for many years. E-mails are routinely backed up on an enterprise's servers and can be accessed—like those of SPE—by malicious parties or disseminated by careless insiders. Moreover, e-mails sent from web-based services such as Gmail, Yahoo!, or Outlook may be stored indefinitely in large numbers in the cloud and may thus exist "without a user's knowledge as an archival or back-up copy."[96]

[43] In 2011, the ABA Standing Committee issued an opinion that

[93] *See* Daniel Miller, *Future of Sony's Amy Pascal Questioned After Hacked Email Revelations*, L.A. TIMES (Dec. 11, 2014, 6:20 PM), http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-sony-amy-pascal-apologizes-20141212-story.html#page=1, *archived at* http://perma.cc/2JAM-JLCY.

[94] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (discussing confidentiality of unencrypted e-mail) (citing David Hricik, *E-mail and Client Confidentiality: Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 479 (1998)).

[95] Bolin, *supra* note 89, at 609.

[96] *See id.*, at 611–12.

qualified its 1999 opinion regarding the propriety of e-mail use.[97] In Formal Opinion 11-459, the ABA Standing Committee concluded that lawyers:

> [S]ending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access.[98]

Opinion 11-459 specifically cautioned lawyers about having their clients communicate with them using an employer's computer or device because employers "often have policies reserving a right of access to employees' e-mail correspondence via the employer's e-mail account, computers or other devices, such as smartphones and tablet devices, from which their employees correspond."[99] Opinion 11-459 also recognized that e-mail subject to access by third parties may compromise a lawyer's ethical duties to preserve client confidences.[100]

B. Lawyers' Use of Web-Based E-mail

[44] Although many lawyers rely on enterprise e-mail systems run by their law firms, other lawyers—particularly those in small to medium size firms—may use web-based e-mail systems such as Gmail, Outlook, Yahoo! Mail, or AOL. Particularly popular is Google's Gmail, which is

[97] *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011) (discussing the duty to protect confidentiality of e-mail communications with clients), *available at* http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/11_459_nm_formal_opinion.authcheckdam.pdf, *archived at* http://perma.cc/UG3HFVCX; *see also* Bolin, *supra* note 89, at 622.

[98] *Id.*

[99] *Id.*

[100] *Id.*

free and offers 1 GB of storage.[101] An analyst estimated 60% of mid-size companies had their e-mail hosted by Google in 2014 and that 92% of startups or very small companies use Google.[102] From the point of view of their ethical obligations, lawyers may have concerns that Google scans e-mails to provide targeted advertising to its users. For example, a lawyer using Gmail to communicate with a client regarding a meeting at a particular hotel may find that she is being targeted with advertisements for that hotel. Although this sort of advertising may be innocuous, there may be greater concerns if advertisements are based on more sensitive content, such as a client's medical condition or employment relationship with a particular company.

1. The Ethics of Gmail

[45] In 2008, the New York State Bar Association Committee on Professional Ethics in Ethics Opinion 820 addressed the question of whether lawyers may use programs that scan e-mails.[103] Although the opinion did not mention Gmail by name, it clearly referenced the service by posing the question of whether "a lawyer [may] use an e-mail service provider that scans e-mails by computer for keywords and then sends or displays instantaneously (to the side of the e-mails in question) computer-generated advertisements to users of the service based on the e-mail communications."[104]

[101] *See Lots of free storage*, GOOGLE, https://www.gmail.com/intl/en_us/mail/help/features.html#storage, *archived at* https://perma.cc/6NDC-NKBC (last modified Apr. 14, 2014) (indicating that users get 15GB of free storage across Gmail, Google Drive, and Google+ Photos).

[102] *See* Dan Frommer, *Google is Stealing away Microsoft's Future Corporate Customers*, QUARTZ (Aug. 1, 2014), http://qz.com/243321/google-is-stealing-away-microsofts-future-corporate-customers/, *archived at* http://perma.cc/WB79-W9LT.

[103] *See* New York State Bar Ass'n Comm. on Prof'l Ethics, Op. 820 (2008) (discussing use of e-mail services that scan e-mail for advertising purposes), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&template=/CM/ContentDisplay.cfm&ContentID=55868, *archived at* http://perma.cc/XB8V-JCGJ.

[104] *Id.*

[46] Ethics Opinion 820 found the "risks posed to client confidentiality [by the e-mail service] are not meaningfully different from the risks in using other e-mail service providers that do not employ this practice" because "no individuals other than e-mail senders and recipients read the e-mail messages."[105] The opinion further stated that the committee would have reached "the opposite conclusion if the e-mails were reviewed by human beings or if the service provider reserved the right to disclose the e-mails or the substance of the communications to third parties without the sender's permission (or a lawful judicial order)."[106]

2. Gmail and Google's Terms of Service

[47] The conclusion that Google's Gmail passes ethical muster because no human being reviews e-mails does not address all the potential risks posed by web-based e-mail services. For example, Ethics Opinion 820 did not discuss the implications that Google's Terms of Service ("TOS"), privacy policies, and other Google statements regarding e-mail privacy have on expectations of privacy in Gmail.

[48] E-mail providers' policies and terms of service have been called "the persistent elephant in the room" regarding e-mail privacy.[107] The current version of Google's TOS—which applies not only to Gmail, but to

[105] *Id.*

[106] *Id.*; *see also* Kevin Raudebaugh, *Trusting the Machines: New York State Bar Ethics Opinion Allows Attorneys to Use Gmail*, 6 WASH. J.L. TECH. & ARTS 83, 90–91 (2010). The Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility also found that the use of Gmail is acceptable. Pennsylvania Bar Ass'n Comm. on Legal Ethics & Prof'l Responsibility, Formal Op. 2011-200 (2011), *available at* http://forctlawyers.com/wp-content/uploads/2012/04/PA-opinion-2011-200.pdf, *archived at* http://perma.cc/U6GM-EEG6 (discussing ethical obligations for attorneys using cloud computing software as a service).

[107] Bolin, *supra* note 89, at 640–41 ("The assumed privacy protections [for e-mail] are now hazy or even hostile to privacy interests, and the assumed practices to keep e[-]mail confidential will obviously depend on the privacy policy. Today's user should be very concerned about the case-specific policies relating to e[-]mail.").

all of Google's "Services," including popular cloud-based products such as Google Apps—contains several provisions that may impact lawyers' expectations of privacy and confidentiality in their communications to clients.[108]

[49] For example, although Google's TOS states that users "retain ownership of any intellectual property rights that [they] hold in . . . content" that is uploaded, submitted, stored, send or received through its services, it also states that users

> [G]ive Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content.[109]

This "license"[110] is "for the limited purpose of operating, promoting, and improving our Services, and to develop new ones."[111]

[50] Regarding targeted advertising, Google's TOS states that "[o]ur automated systems analyze your content (including e[-]mails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored."[112]

[108] *See Google Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms/, *archived at* http://perma.cc/7R26-WU66 (last modified April 14, 2014) [hereinafter *Google Terms of Service*].

[109] *Id.*

[110] *See* Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111, 248–49 (2011) (expressing doubt that a "license" is indeed created through the Google TOS).

[111] *Google Terms of Service*, *supra* note 108.

[51] Google also reserves the right to "suspend or stop a Service altogether," although "where reasonably possible, we will give you reasonable advance notice and a chance to get information out of that Service."[113] Google further disclaims all warranties and reserves the right to "modify these terms or any additional terms that apply to a Service . . . ."[114] Google also warns that it may modify the terms in the future and requests users to "look at [its] terms regularly."[115] If a user does not "agree to the modified terms for a Service, [the user] should discontinue . . . use of the Service."[116]

[52] A lawyer using Gmail may have concerns regarding several aspects of Google's TOS, including the company's unilateral right to "communicate, publish, publicly perform, publicly display and distribute" the content of potentially privileged or confidential e-mails.[117] Although publication is ostensibly for the "limited purpose" of "operating, promoting, and improving our Services, and to develop new ones," the provision is broad enough to encompass several troubling scenarios, including Google's analyzing attorney-client privilege documents to establish a new product aimed at lawyers.[118] Lawyers may also be given pause by the fact that Google can unilaterally suspend services, disclaim all warranties, and place the onus of determining whether the TOS has changed on the users of the service whose only option if they agree with

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Google Terms of Service*, *supra* note 108.

[118] *Id.*

the new TOS is to quit using Gmail.[119]

3. Gmail Users' Expectations of Privacy

[53] Nothing in Google's TOS states that users have any expectation of privacy for the electronic communications they send or receive through Gmail. Indeed, Google has taken the position that individuals sending e-mails to Gmail accounts have no expectation of privacy. When Google was sued in federal court in 2010 for violating state and federal anti-wiretapping laws for intercepting, reading and acquiring the content of e-mails sent or received by Gmail users while the e-mails were in transit, Google argued in a motion to dismiss the complaint that those sending e-mails to Gmail users had consented to Google processing their messages, including accessing the content of messages.[120] Google stated in the motion that

> Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based e-mail today cannot be surprised if their communications are processed by the recipient's E[lectronic] C[ommunication] S[ervice] provider in the course of delivery. Indeed, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[121]

[119] *See* Trope & Hughes, *supra* note 110, at 248–49 (prior Google TOS created an "[i]ncreased [r]isk of [i]nadvertent [g]rant of [l]icense to [c]lient's [i]ntellectual [p]roperty" and raised a "serious ethical risk[] for a law firm or lawyers that use, or allow their staff to use, Google Docs when generating or revising documents that contain client confidential data and content in which the client has intellectual property rights").

[120] *See* Steven Musil, *Google Filing Says Gmail Users Have No Expectation of Privacy*, CNET (Aug. 13, 2013, 7:57 PM), http://www.cnet.com/news/google-filing-says-gmail-users-have-no-expectation-of-privacy/, *archived at* http://perma.cc/EKG4-X9XL.

[121] Defendant Google Inc.'s Motion to Dismiss Plaintiffs' Consolidated Individual and Class Action Complaint at 19, *In re* Google Inc. Gmail Litig., No. 5:13-md-02430-LHK (N.D. Cal. June 6, 2013) (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)),

Google further argued that "the automated processing of e[-]mail is so widely understood and accepted that the act of sending an e[-]mail constitutes implied consent to automated processing as a matter of law."[122]

[54] In rejecting Google's argument, the court found that there was no support for Google's "far-reaching proposition" that users do not have an expectation in privacy when using a web-based e-mail service.[123] The court instead held that senders only "consent[] to the *intended recipient's recording of the e-mail*—not, as has been alleged here, interception by a third-party service provider."[124]

> Google has cited no case that stands for the proposition that users who send e[-]mails impliedly consent to interceptions and use of their communications by third parties other than the intended recipient of the e[-]mail. . . . Accepting Google's theory of implied consent—that by merely sending e[-]mails to or receiving e[-]mails from a Gmail user, a non-Gmail user has consented to Google's interception of such e[-]mails for any purposes—would eviscerate the rule against interception.[125]

available at http://www.consumerwatchdog.org/resources/googlemotion061313.pdf, *archived at* http://perma.cc/J46Z-SZRM.

[122] *Id.*

[123] *See In re* Google Inc. Gmail Litig., No. 13-MD-02430-LHK, 2013 U.S. Dist. LEXIS 172784, at *55–57 (N.D. Cal. Sept. 26, 2013).

[124] *Id.* at 55–56 (emphasis added).

[125] *Id.* at 56. Although Judge Koh rejected many of Google's arguments in its motion to dismiss, she later denied plaintiffs' motion for class certification, finding that many of the issues regarding implied consent were factual in nature and thus created substantial differences among class members. *See In re* Google, Inc. Gmail Litig., No. 13-MD-02430-LHK, 2014 WL 1102660, at *18 (N.D. Cal. Mar. 18, 2014).

[55] Google's argument that those who send e-mails to Gmail users have no expectation of privacy may raise red flags for lawyers using Gmail to make or receive confidential client communications. The fact that Google has not only taken that position but also makes no commitment to preserve the privacy of communications sent through Gmail raises doubts as to whether lawyers using Gmail can reasonably comply with their duty of confidentiality.[126] Although Google—like most companies—has a privacy policy, that policy only restricts the manner in which Google shares personal information with "companies, organizations and individuals *outside of Google*."[127] Google's privacy policy does not restrict *Google's own use* of personal information and is inapplicable to sensitive or confidential information, such as attorney-client communications, that contains no "personal" information.[128]

[56] In arguing that those who send e-mails through Gmail have no expectation of privacy, Google cited the controversial "third party doctrine" set forth in the 1979 case of *Smith v. Maryland*.[129] Under the third party doctrine, an individual voluntarily turning over information to a third party assumes the risk that the third party will turn the information

[126] The protection of users' e-mails by the Electronic Communication Privacy Act (ECPA) and the Stored Communications Act (SCA) of 1986, 18 U.S.C. § 2510 *et seq.* is beyond the scope of this article, but is widely discussed elsewhere. *See, e.g.*, Jacob M. Small, *Storing Documents in the Cloud: Toward an Evidentiary Privilege Protecting Papers and Effects Stored on the Internet*, 23 GEO. MASON U. C.R. L.J. 255, 266 (2013).

[127] *Privacy Policy*, GOOGLE, http://www.google.com/policies/privacy/, *archived at* http://perma.cc/ZGP6-B357 (last modified Dec. 19, 2014) (emphasis added). Google states that it shares personal information with "companies, organizations and individuals outside of Google" only with users' consent, with domain administrators, for external processing, and for legal reasons. *Id.*

[128] *See id.* "Personal information" is defined in Google's Privacy Policy as "information which you provide to us which personally identifies you, such as your name, e[-]mail address or billing information, or other data which can be reasonably linked to such information by Google." *Key Terms*, GOOGLE, http://www.google.com/policies/privacy/key-terms/, *archived at* http://perma.cc/Z7VR-37X5 (last visited Jan. 5, 2015).

[129] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

over to another party and thus has no expectation of privacy in the information.[130] As argued by Google (but rejected by the district court), Gmail users may not have an expectation of privacy or confidentiality in e-mail messages because Google reserves the right to access or "process" the e-mails.

[57] Although the Supreme Court has yet to address applicability of the third party doctrine to the digital world, it may have an opportunity to do so in the context of challenges to the National Security Agency's mass collection of telephony metadata that was the centerpiece of Edward Snowden's 2013 revelations regarding NSA practices.[131] The two federal courts that have addressed the constitutionality of the NSA's program to date have reached opposite results.[132]

4. E-mail Security Risks.

[58] Although some lawyers may not be concerned about Google's reliance on the third party doctrine (which was rejected by the court in the Gmail litigation), they may nonetheless have concerns regarding the more general security risks posed by unauthorized distribution of confidential e-mails by insiders and outsiders. Because e-mail can be readily forwarded either deliberately or accidentally to third parties, it is far less secure than

[130] *See id.* at 743–44.

[131] *See* THE WHITE HOUSE, ADMINISTRATION WHITE PAPER BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT (2013), *available at* http://big.assets.huffingtonpost.com/Section215.pdf, *archived at* http://perma.cc/7YMA-7ZAN.

[132] In *Klayman v. Obama*, the court found that the program was unconstitutional because technological advances have made the third party doctrine inapplicable. Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C. 2013). A week later, the court in *American Civil Liberties Union v. Clapper* reached the opposite conclusion. American Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013); *see also* Jack Lerner et al., *The Duty of Confidentiality in the Surveillance Age*, 17 J. INTERNET L., Apr. 2014, at 17 (arguing that lawyers' duty of confidentiality may be compromised by NSA programs and that "NSA surveillance revelations require attorneys to re-evaluate the security of communications over the Internet and 'in the cloud.'").

using postal services—as the SPE executives discovered when their embarrassing e-mails were revealed by hackers.[133] Although mail may be misaddressed or misdelivered, there is no "reply all" button for postal mail, nor is it generally subject to being stolen by malicious outsiders.

[59] As earlier discussed, hackers often use social engineering techniques, including "spear-fishing," which is typically delivered through e-mails, to try to obtain valuable or confidential information. Through these techniques, hackers may gain access not only to e-mails, but to documents containing personal, proprietary or confidential information in the entire computer system.[134]

[60] The security of e-mail also rests to a large extent on the security of passwords, which offer little protection against hackers. Like other forms of personal information, hackers are interested in passwords because they provide a means to access banking and retail accounts. Because many individuals use the same password for several accounts, hackers seek users' passwords either through "phishing" or hacks of large numbers of stored passwords. For example, a hack in 2013 of the online dating service Cupid Media "exposed more than 42 million consumer records, including names, e[-]mail addresses, unencrypted passwords and birthdays . . . ."[135] In 2012, a Russian hacker site posted 6.5 million passwords hacked from LinkedIn.[136] The "Heartbleed" bug in 2014 infected the technology that encrypts communications with websites and exposed millions of passwords.[137]

[133] *See* Miller, *supra* note 93.

[134] *See* Danhieux, *supra* note 30; Cooney, *supra* note 20.

[135] Brian Krebs, *Cupid Media Hack Exposed 42M Passwords*, KREBS ON SECURITY (Nov. 20, 2013), http://krebsonsecurity.com/2013/11/cupid-media-hack-exposed-42m-passwords/, *archived at* http://perma.cc/S69D-UHPN.

[136] *See* Sara Gates, *LinkedIn Password Hack: Check to See if Yours Was One of the 6.5 Million Leaked*, HUFFINGTON POST (June 7, 2012, 11:25 AM), http://www.huffingtonpost.com/2012/06/07/linkedin-password-hack-check_n_1577184.html, *archived at* http://perma.cc/HS5F-VEX3.

[61] The evolving security threats to e-mail undermine the assumptions of prior opinions finding that e-mail is an ethical means of communicating client confidential information. As with all technology, lawyers must base their considerations of what is reasonable to preserve client confidences not on past parameters, but on the current state of technology and security risks.[138] Because of current security concerns, lawyers should consider whether the use of unencrypted e-mail for sensitive and confidential communications fulfills their ethical duties.

VI. LAWYERS' USE OF CLOUD COMPUTING SERVICES

[62] "Cloud computing" is a vague and frequently misunderstood marketing term. For example, in a recent *Dilbert* cartoon the perennial malingerer Wally told the "Pointy Haired Boss," "[i]f you need me, I'll be in the cloud fixing a software issue." He also told his boss that because "[t]here's no cell coverage in the cloud, so it might seem to you as if I am at home doing nothing."[139]

[63] In point of fact, the "cloud" is not located in the sky (or in Wally's home) but is instead a name for the outsourcing of computing functions through servers owned by "cloud computing providers" and not by companies themselves.[140] Customers, including law firms, realize benefits from such outsourcing, including cost savings that "allow businesses to avoid the burden of the security and management responsibilities associated with data storage, as well as the complexities of maintaining the

[137] *See* Brian Krebs, *"Heartbleed" Bug Exposes Passwords, Web Site Encryption Keys*, KREBS ON SECURITY (Apr. 8, 2014), http://krebsonsecurity.com/2014/04/heartbleed-bug-exposes-passwords-web-site-encryption-keys/, *archived at* http://perma.cc/4CM7-RP8M.

[138] *See* Bolin, *supra* note 89, at 622.

[139] Scott Adams, *Comics*, DILBERT (Dec. 8, 2014), http://www.dilbert.com/2014-12-08/, *archived at* http://perma.cc/G8L6-P5MQ.

[140] *See* Kenneth L. Bostick, *Pie in the Sky: Cloud Computing Brings an End to the Professional Paradigm in the Practice of Law*, 60 BUFF. L. REV. 1375, 1381–82, 1384–85 (2012).

infrastructure under which the data is held."[141]

[64] According to the working definition of the National Institute of Standards and Technology (NIST), "[c]loud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." [142] There are several varieties of cloud computing services, including: cloud software as a service (SaaS), which allows users to run software through a cloud infrastructure; cloud platform as a service (PaaS), which allows users to run their own applications using the programming language provided by the service; and cloud infrastructure as a service (IaaS), which allows "the consumer . . . to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications."[143]

[65] The most frequent law firm uses of the cloud are running software applications (such as word processing, spreadsheets, and accounting) and storing documents. For example, lawyers, like other consumers, may use Amazon's Simple Storage Service (Amazon S3) to store documents,[144] or Google's Docs, Sheets and Slides (available through Google's web browser Chrome) to create documents, spreadsheets and presentation slides.[145] Such services are generally referred to as "public clouds," in

[141] *Id.* at 1376; *see also* Trope & Hughes, *supra* note 110, at 164–65 (describing the history of use of cloud services); Woods, *supra* note 5 (describing the exponential growth of cloud computing services in recent years).

[142] PETER MELL & TIMOTHY GRANCE, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), *available at* http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf, *archived at* http://perma.cc/ENM9-B4MQ.

[143] Trope & Hughes, *supra* note 110, at 168.

[144] *See Amazon S3*, AMAZON, https://aws.amazon.com/s3/, *archived at* https://perma.cc/2L3D-5TED (last visited Feb. 7, 2015).

other words, services offered to the general public.[146] In addition, law firms may also use free document sharing services—such as Dropbox or Box—for a wide variety of purposes.[147]

[66] Law firms also make use of "private clouds," which are off-site servers not generally available to the public which the firm pays a third party to manage.[148] Law firms use private clouds for wide variety of services, including accounting, software, and storage of documents.[149] Although the following discussion concentrates on the use of the public cloud, it applies in certain respects—including security and control issues—to private clouds.

A. Ethics of Lawyers' Use of Public Cloud Computing Services

[67] Bar organizations have generally concluded that lawyers may entrust confidential documents to cloud computing providers if certain conditions are met. The nineteen different state bodies[150] that have

[145] *See Edit Office Files in Google Docs, Sheets, and Slides*, GOOGLE, https://support.google.com/docs/answer/6049100?hl=en, *archived at* https://perma.cc/35UT-4WTP (last visited Feb. 7, 2015).

[146] *See* Trope & Hughes, *supra* note 110, at 170.

[147] *See Law Firm File Sharing in 2014*, LEXISNEXIS 6 (May 28, 2014), *available at* http://www.slideshare.net/BusinessofLaw/lexisnexis-2014-survey-of-lfile-sharing-survey-report-final, *archived at* http://perma.cc/Z8KM-WAK6. The report also found that lawyers were often unaware of whether other lawyers in their firm used file-sharing services. *Id.* at 7.

[148] *See* Trope & Hughes, *supra* note 110, at 170.

[149] *See* Stephanie L. Kimbro & Tom Mighell, *Popular Cloud Computing Services for Lawyers: Practice Management Online*, L. PRAC. MAG., Sept./Oct. 2011, *available at* http://www.americanbar.org/publications/law_practice_magazine/2011/september_october/popular_cloud_computing_services_for_lawyers.html, *archived at* http://perma.cc/WEW7-2HWS (listing numerous cloud applications available to lawyers).

reviewed the issue to date have found cloud computing ethical if lawyers "take reasonable steps to ensure that their law firm's confidential data is protected from unauthorized third party access."[151]

[68] For example, Iowa Ethics Opinion 11-01, which addressed issues of confidentiality in the cloud, concluded that

> A lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.[152]

[150] *See Cloud Ethics Opinions Around the U.S.*, ABA, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html, *archived at* http://perma.cc/TJU8-JQF2 (last visited Jan. 5, 2015).

[151] Nicole Black, *The Ethics of Cloud Computing for Lawyers*, ABA (2012), *available at* http://www.americanbar.org/publications/gpsolo_ereport/2012/september_2012/ethics_cloud_computing_lawyers.html, *archived at* http://perma.cc/B285-7NAD; *see also* Thomas G. Wilkinson Jr., *Ethics Digest*, 34 PA. LAW. 49, 49 (2012) (discussing Pennsylvania Bar Association Legal Ethics and Professional Responsibility Committee Formal Opinion 2011–200); Robert Ambrogi, *Cloud Ethics Opinions: A Full List (Maybe)*, LAW SITES BLOG (May 23, 2014), http://www.lawsitesblog.com/2014/05/cloud-ethics-opinions-full-list.html, *archived at* http://perma.cc/5SLB-W8WR.

[152] Letter from Nick Critelli, Comm. Chair, Iowa State Bar Ass'n Ethics & Practice Guidelines Comm., to Dwight Dinkla, Exec Dir. Iowa State Bar Ass'n (Sept. 9, 2011) (quoting Iowa R. of Prof'l Conduct 32:1.6), *available at* http://www.wicsec.org/wp-content/uploads/2011%20WICSEC%20Conference%20Materials/M-6%20Iowa%20Bar%20Ethics%20Opinion%209911%20-%20Worley,%20Peiper.pdf, *archived at* http://perma.cc/NTS7-5CAH; Black, *supra* note 151 (analyzing Iowa State Bar Association's opinion).

[69] Opinion 842 of the New York State Bar Association Committee on Professional Ethics similarly addressed the ethical propriety of cloud computing.[153] Opinion 842 concluded that use of online systems to store confidential information implicated Rule 1.6's confidentiality requirement, but found that a lawyer can use a cloud service to store client files "provided that the lawyer takes reasonable care to ensure that the system is secure and that client confidentiality will be maintained."[154]

[70] Opinion 842 found that necessary "[r]easonable care . . . may include consideration" of four issues:

> (1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;
> (2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;
> (3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or
> (4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.[155]

[153] *See* New York State Bar Comm. on Prof'l Ethics, Op. 842 (2010), *available at* http://old.nysba.org/AM/Template.cfm?Section=Ethics_Opinions&ContentID=140010&template=/CM/ContentDisplay.cfm, *archived at* http://perma.cc/P6P8-CJKR (using outside online storage provider to store client confidential information).

[154] *Id.*

[155] *Id.*

[71] Opinion 842 cautioned that "[t]echnology and security of stored data are changing rapidly" and that "the lawyer should periodically reconfirm that the provider's security measures remain effective in light of advances in technology."[156] The lawyer also has the duty, if he or she learns that security measures are ineffective, to "investigate whether there has been any breach of his or her clients' confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated."[157] Lawyers must also monitor the law relating to technology, which "is changing rapidly," to see "when using technology may waive an otherwise applicable privilege."[158]

[72] New York Opinion 842 echoes the approach to technology taken in California Ethics Opinion 2010-179.[159] Although the California opinion dealt with the propriety of a lawyer using public and home wireless technology, its conclusion that lawyers must be cognizant of the effect of changing technology and security threats is equally applicable to cloud computing. As Opinion 2010-179 states, "[t]he greater the sensitivity of the information, the less risk the attorney should take with technology. If the information is of a highly sensitive nature and there is a risk of disclosure when using a particular technology, the attorney should consider alternatives unless the client provides informed consent."[160] Moreover, "if a particular technology lacks essential security features, use

[156] *Id.*

[157] *Id.*

[158] *Id.* (citing City of Ontario v. Quon, 560 U.S. 746, 762–63 (2010) (dealing with expectations of privacy in mobile technology as an example of changes that may affect privilege)).

[159] *See* Trope & Hughes, *supra* note 110, at 192–93.

[160] State Bar of California Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2010-179 (2010), *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836, *archived at* http://perma.cc/4BKQ-HL3Z.

of such a technology could be deemed to have waived [attorney-client] protections. Where the attorney-client privilege is at issue, failure to use sufficient precautions may be considering in determining waiver."[161]

B. Security Risks of Lawyers' Use of Public Cloud Computing Services

[73] Although the California, Iowa and New York ethics opinions require lawyers to assess—and continue to assess—the security features of cloud computing providers, lawyers may have difficulties in fulfilling this obligation with major public cloud providers. As with e-mail, the standard policies of many public cloud providers—including Amazon and Google—make it challenging for lawyers to determine whether these services have the security measures required by ethics opinions.

[74] For example, Google's TOS states that Google provides its services "using a commercially reasonable level of skill and care."[162] Notwithstanding this commitment, Google's TOS states (in all capital letters) "NEITHER GOOGLE NOR ITS SUPPLIERS OR DISTRIBUTORS MAKE ANY SPECIFIC PROMISES ABOUT THE SERVICES. FOR EXAMPLE, WE DON'T MAKE ANY COMMITMENTS ABOUT THE CONTENT WITHIN THE SERVICES, THE SPECIFIC FUNCTIONS OF THE SERVICES, OR THEIR RELIABILITY, AVAILABILITY, OR ABILITY TO MEET YOUR NEEDS. WE PROVIDE THE SERVICES 'AS IS.'"[163] Google also excludes all warranties and further states (again in all capital letters) "WHEN PERMITTED BY LAW, GOOGLE AND GOOGLE'S SUPPLIERS AND DISTRIBUTORS, WILL NOT BE RESPONSIBLE FOR LOST PROFITS, REVENUES, OR DATA, FINANCIAL LOSSES OR INDIRECT, SPECIAL CONSEQUENTIAL, EXEMPLARY, OR

[161] *Id.*; *see also* Trope & Hughes, *supra* note 110, at 192–93 (discussing the applicability of ethical opinions to cloud computing).

[162] *Google Terms of Service*, *supra* note 108.

[163] *Id.*

PUNITIVE DAMAGES."[164]

[75] Under the heading "Business uses of our Services," Google's TOS states that a "business accepts these terms" and

> [W]ill hold harmless and indemnify Google and its affiliates, officers, agents, and employees from any claim, suit or action arising from or related to the use of the Services or violation of these terms, including any liability or expense arising from claims, losses, damages, suits judgments, litigation costs and attorneys' fees.[165]

[76] Google's TOS also incorporates the company's privacy policy,[166] which includes a section on "information security" stating that, generally, "[w]e work hard to protect Google and our users from unauthorized access to or unauthorized alteration, disclosure or destruction of information we hold."[167] Google's privacy policy also states that it encrypts certain services using Secure Sockets Layer (SSL), offers two step verification and a safe browsing feature in Google Chrome, and reviews its "information collection, storage and processing practices, including physical security measures, to guard against unauthorized access to systems."[168] Finally, Google restricts "access to personal information to Google employees, contractors and agents who need to know that information in order to process it for us, and who are subject to strict contractual confidentiality obligations and may be disciplined or terminated if they fail to meet these obligations."[169]

[164] *Id.*

[165] *Id.*

[166] *Id.*

[167] *Privacy Policy*, *supra* note 127.

[168] *Id.*

[169] *Id.*

[77] Google's TOS and Privacy Policy do not provide any means for an attorney using Google's services to measure or assess the company's protection of confidential information stored or processed through the services. Not only does Google expressly decline to make any specific promises about its services—including the security of information stored on Google servers—it also requires business users to indemnify Google for any lawsuits "arising from or related to the use of the Services."[170]

[78] Google's Privacy Policy also makes no commitments regarding security of customers' information. Indeed, whatever restrictions the privacy policy places on dissemination of information are restricted to "personal information,"[171] which is a considerably narrower category than information that lawyers may consider to be confidential. Google's "license" to the content of documents stored on its servers and its right to make "derivative works" are also troublesome from the point of view of maintaining client confidentiality for information stored on Google's services.[172]

[79] Amazon similarly limits its liability for its "cloud drive," which provides remote storage for documents, by stating that

> (a) in no event will our or our software licensors' total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) arising

[170] *Google Terms of Service*, *supra* note 108.

[171] *See Key Terms*, *supra* note 128 (defining "personal information" as "information which you provide to us which personally identifies you, such as your name, e[-]mail address or billing information, or other data which can be reasonably linked to such information by Google.").

[172] *See* Trope & Hughes, *supra* note 110, at 248–50 ("There are probably few, if any, clients that would be willing to agree to grant a cloud vendor a right to any content that the client may generate or that its attorneys may generate through the use of a cloud-based, word-processing program such as Google Docs. A lawyer or law firm would certainly also be unwilling to agree to grant such a license.").

> out of or related to your use or inability to use the Software exceed the amount of fifty dollars ($50.00);
> (b) in no event will our total liability to you for all damages arising from your use of the Service or information, materials or products included on or otherwise made available to you through the Service (excluding the Software), exceed the amount you paid for the Service related to your claim for damages; and
> (c) we have no liability for any loss, damage or misappropriation of Your Files under any circumstances or for any consequences related to changes, restrictions, suspensions or termination of the Service or the Agreement. These limitations will apply to you even if the remedies fail of their essential purpose.[173]

Cloud service providers like Google and Amazon also make it difficult for attorneys to assure that they will be informed by the providers of any breach of security in the system. Under Google and other providers' TOS, there is "no assurance that a customer would be given any explanation of faults in the system."[174] Moreover, most public cloud computing providers, like Amazon and Google, make no commitments regarding the preservation and retrieval of documents from their services nor do they affirmatively state that they will provide information to users about security compromises.[175] "It is, therefore, questionable whether a lawyer or law firm who relinquishes control over the storage of its data would be acting reasonably when it has little to no control over security breaches."[176] Because state data breach notification laws pertain only to personal data, there is no legal obligation for public cloud providers to

[173] *Amazon Cloud Drive Terms of Use*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?nodeId=201376540, *archived at* http://perma.cc/KJX3-GMVS (last updated Nov. 11, 2014).

[174] Trope & Hughes, *supra* note 110, at 201–02.

[175] *See id.* at 206–07 (noting that Amazon's agreement removed any such assurances).

[176] *Id.* at 220–21.

provide notice to users regarding compromise of non-personal data such as confidential documents stored on a service.[177]

[80] Cloud computing also entails more general security concerns. A 2010 article by Christopher Soghoian argues that security concerns are inherent to cloud computing and thus "render[] the cloud computing model fundamentally unfit for the practice of law."[178] These "inherent" risks include transmittal of user names and passwords to servers via unencrypted network connections, transmittal of data that "'can easily be snooped on by hackers'" and encryption that is restricted to initial login information.[179] The Cloud Security Alliance has also assembled a list of the top nine security risks to the cloud: "(1) [d]ata [b]reaches; (2) [d]ata [l]oss;" (3) account [or service traffic] hijacking; (4) insecure [interfaces and] APIs; "(5) [d]enial of [s]ervice; (6) [m]alicious [i]nsiders; (7) [a]buse of [c]loud [s]ervices; (8) [i]nsufficient [d]ue [d]iligence;" and "(9) [s]hared [t]echnology [i]ssues."[180] Although these threats are not unique to the cloud, they demonstrate that lawyers do not avoid security issues when using the cloud any more than they do with their own in-house computing services.

VII. LAWYERS' USE OF E-MAIL, CLOUD COMPUTING, AND TECHNOLOGY

[81] Given the security challenges to confidential information sent through e-mails or stored with public cloud providers, lawyers should exercise greater care using these technologies than they have done in the

[177] *See id.* at 219–21.

[178] Bostick, *supra* note 140, at 1380.

[179] *Id.* at 1395–96 (citing Christopher Soghoian, *Caught in the Cloud: Privacy, Encryption, and Government Back Doors in the Web 2 0 Era*, 8 J. TELECOMM. & HIGH TECH. L. 359, 372 (2010)).

[180] CLOUD SECURITY ALLIANCE, THE NOTORIOUS NINE: CLOUD COMPUTING TOP THREATS IN 2013 6–7 (2013), *available at* https://downloads.cloudsecurityalliance.org/initiatives/top_threats/The_Notorious_Nine_Cloud_Computing_Top_Threats_in_2013.pdf, *archived at* https://perma.cc/KBX2-A7R4.

past. Although ethics bodies have approved the use of both e-mail and cloud computing, they have done so with the important proviso that lawyers must reassess the propriety of using the technologies as both the technology and security risks continue to evolve. What may have been "reasonable" security in the past may no longer be adequate. Given risks of exposure of confidential documents and e-mails—as exemplified by the SPE breach—lawyers should consider whether it is appropriate to entrust highly confidential client information to unencrypted e-mail and cloud services.

[82] Although encryption is increasingly inexpensive and is used in many businesses, it is not yet widely used by lawyers.[181] But as lawyers come to understand the inherent security risks in e-mail and in cloud computing, they should consider using encryption, particularly for e-mails and documents containing sensitive information, such as client confidential documents and protected health information under HIPAA.[182]

[83] Like their clients, lawyers must put their own houses in order by implementing security measures and incident responses plans for security incidents and their aftermath.[183] A key aspect of security preparedness is training law firm personnel, including lawyers themselves. Even senior partners are not immune to phishing attacks and misuse of public document sharing sites—such as Dropbox or Box—which are "built to handle consumer data, with no true security safeguards, no ability to audit,

[181] *See Law Firm File Sharing in 2014*, *supra* note 147, at 1 (indicating that 89% of firms reported using e-mail and 74% use it on a daily basis, but that lawyers generally do not use encryption and instead use confidentiality statements in the e-mails); Scott Aurnou, *Lawyers and Email: Ethical & Security Considerations*, SECURITY ADVOCATE (July 8, 2014), http://www.thesecurityadvocate.com/2014/07/08/lawyers-and-email-ethical-security-considerations/, *archived at* http://perma.cc/9A5T-4RU3 (noting that confidentiality statements "essentially do[] nothing to protect firm or client data from any nefarious actors who view it . . . .").

[182] *See* Aurnou, *supra* note 181.

[183] *See id.* (discussing the need of lawyers and law firms to put in place security response plans).

and no redundancy or backups."[184]

[84] Law firms should also assess whether they need to put into place policies and procedures prohibiting certain practices that increase the danger of dissemination of confidential information. These policies may encompass topics such as using public cloud providers or file sharing services for sharing documents, the use of web-based e-mail services, and use of public cloud computing providers for sensitive documents. Instead of using public cloud services, lawyers might use "enterprise-grade file sharing services that focus on the security and protections designed with law firms in mind."[185] As earlier noted, if lawyers do use public storage or file sharing services, they should consider using encryption for confidential or proprietary documents.[186]

[85] Given recent ethical opinions, it is clear that lawyers must also continue to keep abreast of security risks posed by technology to fulfill their duties of competence and confidentiality. Although not every lawyer must be a specialist in technology, the days when some in the profession could afford to be technophobes are over. Like their clients, lawyers share the burden of preserving sensitive and proprietary data against attacks and unauthorized exposure.

[184] Bobby Kuzma, *Security in Era of Mobile Devices and Cloud Computing, in* 14 PRACTICE INNOVATIONS 15 (2013), *available at* https://info.legalsolutions.thomsonreuters.com/signup/newsletters/practice-innovations/2013-jan/Jan13_PracticeInnovations.pdf, *archived at* https://perma.cc/Q5UK-6GD5.

[185] *See Law Firm File Sharing in 2014*, *supra* note 147, at 9 (finding that 64.9% of firms do not provide an enterprise-grade filing service.).

[186] *See* Aurnou, *supra* note 181 (noting that DropBox and Google Drive are not suitable options for lawyers).