I. INTRODUCTION

Bring-your-own-device ("BYOD") is an approach to mobile technology that permits access to a company's computer network and email system through employee-owned mobile devices. BYOD permits employees to use the same device for both personal and business purposes. The wide-spread adoption of BYOD programs has been described as "the most radical change to the economics and the culture of client computing in business in decades." More than half of all employees use their personal mobile technology for work.

The BYOD trend has slowly made its way to the legal profession. BYOD has become a viable option for lawyers and law firms for several reasons. First, it theoretically limits a law firm's capital outlays and investment costs as the firm's lawyers purchase the devices on their own. Since no one prefers to carry multiple devices, a BYOD approach to technology permits the consolidation of devices. It provides a convenient option for managing personal and professional information, especially when lawyers are outside the office.


3 Joshua Poje, Security Snapshot: Threats and Opportunities, in ABA TECHREPORT 2013 (2013), available at http://www.americanbar.org/publications/techreport/2013/security_snapshot_threats_and_opportunities.html (reporting that 34% of the respondents to the ABA’s 2013 legal technology survey "reported that their firms allowed them to connect their personal mobile devices to the network without restriction") (emphasis in original).

4 At least one study, however, suggests that a BYOD approach will actually result in higher costs. See Tom Kaneshige, BYOD If You Think You're Saving Money, Think Again, CIO, (Apr. 4, 2012, 8:00 AM), http://www.cio.com/article/2397529/consumer-technology/byod--if-you-think-you-re-saving-money--think-again.html (discussing a study by the Aberdeen Group of a company with 1,000 mobile devices which concluded that the company spent "an extra $170,000 per year, on average, when they use a BYOD approach").
Because it allows employees to work with a device or a platform they know and may prefer to use, BYOD evangelists suggest that its adoption improves efficiency. BYOD proponents also claim it gives "employees the freedom to work and collaborate the way they prefer making for a more mobile, productive, and satisfied workforce."\(^5\)

With the development of wearable devices such as smart watches, smart jewelry, and Google Glass, as well as health or fitness sensors that are designed to communicate with apps on a mobile device, they are quickly becoming the center of an individual's personal area network ("PAN").\(^6\)

The proliferation of mobile devices, however, trigger a number of unique risks for lawyers and law firms, especially in light of our ethical obligation to competently safeguard client information under the Model Rules of Professional Conduct. Superimposed on a lawyer's ethical duty to safeguard client information is the statutory obligation imposed by state and federal laws and regulations to protect various categories of personally identifying information, non-public financial information and protected health information.

Mobile devices permit lawyers and staff to engage in social networking around the clock. One of the hidden risks of social media activity, however, is that the information posted on social media sites by lawyers and staff frequently can provide ample information for cyber criminals to develop sophisticated spear phishing schemes directed at law-firm personnel.

BYOD limits a law firm's ability to control the use of these devices in the same fashion it controls the use of computers and equipment owned and supplied by the firm. In an environment where mobile devices are corporately owned and supplied, a law firm has complete control of the type of devices permitted to access its network, can mandate the use of strong passwords to access the device, ensure the device is locked out after a short period of inactivity or after a certain number of failed attempts to log onto the device, limit how the phone or device can be used, ensure the device is encrypted, lock down the device's browser, limit the user's ability to visit malicious or suspicious websites, provide a whitelist of applications that could be downloaded on the device or a blacklist of applications prohibited on the device, ensure that the latest endpoint security is available and remotely wipe the device if it is lost or stolen. In an

---


unregulated BYOD environment, many of these responsibilities are transferred to the device's owner. As a result, clients in some industries are pushing back against law firm BYOD strategies.7

A mobile device that becomes infected with malware can serve as a launching pad for an attack on the firm's network and potentially place both client and firm information at risk. An unprotected device that is lost or stolen can trigger a reporting obligation if the device contained or provided access to certain categories of unencrypted information.

A law firm's failure to have a comprehensive BYOD policy is a prescription for disaster. An ill-conceived BYOD policy, one that is not disseminated throughout the firm,8 or one that is not routinely enforced, complicates a law firm's ability to safeguard client and firm information.

This article will outline the ethical risks triggered by BYOD and provide suggestions towards developing a comprehensive data security policy for mobile devices that will help mitigate the risks posed by the adoption of a BYOD approach to mobile technology. Part II addresses the impact of technology on the legal profession and discusses how technology has fundamentally altered the delivery of legal services. Part III reviews the lawyer's duty of competence and addresses how that duty includes knowing the risks and benefits of technology and what that ethical duty entails. Part IV outlines the various risks triggered by the adoption of a BYOD approach to mobile technology. Part V addresses a lawyer's ethical duty to safeguard information and communications against technology-based risks and Part VI outlines a law firm's obligation to have measures in place that provide reasonable assurance that its lawyers are conforming to the Rules of Professional Conduct and that the conduct of its non-lawyer assistants is compatible with those professional obligations. Part VI also includes a discussion of ethics opinions addressing cloud computing because mobile devices and the cloud go hand-in-hand. Part VII of this article provides recommendations for law firms adopting a BYOD approach to mobile technology, and concludes with a sample policy addressing data security for mobile devices in Part VIII.


8 Poje, supra note 3 (noting 13% of lawyers responding to the ABA's 2013 legal technology survey did not know "if their firm had any technology polices in place" and noting "the widest knowledge gap is among younger law firm attorneys," including "29% of associates" and "21% of attorneys under the age of 40").
II. THE IMPACT OF TECHNOLOGY ON THE LEGAL PROFESSION

Relentless advances in technology have fundamentally altered the delivery of legal services. Technology provides lawyers the ability to remotely practice from any location, and has cut the tether that traditionally bound lawyers to the bricks and mortar of a law firm. It has made the virtual law office a reality.9

Technology has also altered how we interact and communicate with our clients, third parties and one another. Text messaging and email have relegated written notes and letters to the horse and buggy era. Communications are more immediate and less formal than ever before. Social media has further blurred the line between our personal and professional lives and provides another means to virtually connect with anyone at anytime from anywhere.

At one time, law firms could protect information in their possession the same way kings protected their castle in the Middle Ages – by building a strong perimeter. Rather than a moat with a drawbridge and high stone walls, locks on doors and file cabinets and a clean desk policy provided the necessary protection. When the Internet came into use, a firewall was added to the law firm’s perimeter defenses. Once technology became mobile, however, the perimeter of the "castle's walls" became much harder to defend.

The mobility of modern technology has made protecting client information a far more complex and difficult task for lawyers and law firms than ever before. Innovative communication and file sharing technologies, wireless internet connections, the growing popularity of cloud computing, and the proliferation of mobile devices have significantly complicated the ethical duties and the statutory obligations imposed upon lawyers to protect information entrusted to them.10 "Nearly ubiquitous connectivity disperses nearly ubiquitous vulnerability."11


10 In 1996 Congress enacted the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), which set a federal privacy floor for personally identifying information in health records. Subsequently, in 2009 Congress adopted the Health Information Technology for Economic and Clinical Health Act (“HITECH Act”), Pub. L. No. 111-5, Div. A, Title XIII, Div. B, Title IV, 123 Stat. 226, 467 (2009), which among other things, extended the HIPAA obligations of physicians, hospitals, group health plans and other “covered entities” to protect PHI (“protected health information”) to “business associates.” The HITECH Act's final regulations were published in January 2013 as the HIPAA Omnibus Final Rule (“Omnibus Rule”). Business associates were given until September 23, 2013 to comply with the Omnibus Rule. A lawyer or law firm that receives, transmits, uses or maintains PHI in the
The advent of consumer file-sharing technologies like Dropbox, SugarSync, and Beehive, and cloud-based software through which information can be readily transferred outside the firm network has rendered the "castle's" perimeter defenses illusory. Technology provides the means to bypass locked doors and filing cabinets and circumvent traditional methods used to protect confidential information and communications.

Technology also brings hackers to the doorstep of every law firm. In November of 2011, the FBI held a meeting with 200 law firms in New York where it explained that hackers consider law firms to be the "back door to the valuable data of their corporate clients." Mandiant, a cyber-security firm, estimated that in 2011 at least 80 major law firms in the U.S. had been hacked. Hackers and cyber criminals target law firms for two reasons: the perception that law firms’ cyber defenses are weaker than that of their clients, and the concentration of valuable information firms accumulate. As a result, the computer networks of law firms are frequently probed for vulnerabilities, and

course of providing legal services to a covered entity or another business associate generally qualifies as a business associate under HIPAA and must comply with its applicable privacy and security requirements.


12 See, e.g., Debra Cassens Weiss, Suit Claims Ex-Partner Installed Software Allowing Continued Access to Law Firm Files, ABA JOURNAL (Feb. 13, 2012, 1:31 PM CST), http://www.abajournal.com/news/article/suit_claims_expartner_installed_software_allowing_continued_access_to_law_/ (addressing a lawsuit brought against a former partner of a law firm who allegedly downloaded Dropbox onto the firm's network to continue accessing files via the Cloud following his departure from the firm).


14 Id.

15 Ed Finkel, Cybersapce Under Siege, ABA JOURNAL (Nov. 1, 2010, 9:58 AM CDT), http://www.abajournal.com/magazine/article/cyberspace_under_siege/("Law firms have tremendous concentrations of really critical private information' ... and breaking into a firm's computer system 'is a really optimal way to obtain economic and personal security information." (quoting Bradford A. Bleier, unit chief to the Cyber National Security Section in the FBI's Cyber Division)).

16 Matthew Goldstein, Wall St. Is Told to Tighten Digital Security of Partners, N.Y. TIMES, April 8, 2015, http://www.nytimes.com/2015/04/09/business/dealbook/wall-st-is-told-to-tighten-digital-security-of-partners.html?_r=0 (noting "law firms were a logical target for hackers because they are rich repositories for confidential data").
hackers are routinely sending socially engineered emails to lawyers with attachments containing malware or links to malicious web sites.

While hackers’ motives are understood and their attack strategies are known, preventing successful hacks has proven to be difficult. The unfortunate reality is that many successful security breaches could have been avoided if a vulnerability had been timely patched, or if an employee had simply avoided clicking on a link in an email from a person he or she did not know. While data breaches resulting from malicious hackers have grabbed headlines, more data breaches are the result of human error, lost or stolen mobile devices, bad disposal practices and computer glitches than the work of hackers. Confidential information can be compromised simply by misaddressing an email or by clicking "reply to all." While there are technological solutions that can strengthen a law firm’s defenses, frequently the weakest link in the security of a law firm is its personnel.

Further complicating matters is that cyber threats are constantly evolving. Spam filters will capture some phishing emails and anti-virus protection will recognize off-
the-shelf forms of malware, but hackers are developing new methods to evade those filters and are refining malware to avoid detection. Malware is now designed to specifically target mobile devices. As a result, constant vigilance is required, and security measures must adapt as new threats emerge.

There is no “one size fits all” approach to how law firms protect the information in their possession. Variables such as a law firm’s size, its culture, geographic footprint, office structure, practice areas, technological sophistication and available resources are factors that influence a law firm's approach to protecting the information in its possession.

While ethical discussions involving protecting client information and cyber security frequently focus on available technological tools, even the best technological defenses are no guarantee against a data breach. Rather, a holistic approach to data protection and cyber security is required. Security experts recommend layers of protection or "defense in depth." Because no technological solution is foolproof, coordinated technical, administrative and physical safeguards are needed to protect information. Robust technical, administrative and physical safeguards a law firm puts in place to protect client information, however, can be bypassed by employee carelessness or refusal to follow the firm's security protocols. As a result, any discussion of the duty to protect information should not overlook physical and administrative safeguards to protect information, the education and training of lawyers and staff on the firm's security measures, and consistent discipline if those security measures are violated.

III. A LAWYER'S DUTY OF COMPETENCE REQUIRES KNOWING THE RISKS AND BENEFITS OF TECHNOLOGY

A lawyer's fundamental ethical duty is to provide competent representation to a client. This "requires the legal knowledge, skill, thoroughness and preparation reasonably necessary" for the engagement. The Model Rules of Professional Conduct were modified in 2012 to confirm that a lawyer's duty of competence includes knowing


23 See, e.g., Cal. State Bar, Formal Op. 2012-184, n.8 (2012) (noting a lawyer, "may employ the most up-to-date security precautions for his server," but would nonetheless violate the obligation to take reasonable precautions to protect client information if he "fail[ed] to lock the door to his office, thereby allowing anyone to come in and rifle through his clients' paper files").

the risks and benefits associated with the technology used by a lawyer in the delivery of legal services.\textsuperscript{25} While various state ethics opinions had previously addressed technology issues,\textsuperscript{26} the Model Rules had not, and the 2012 amendments to the Model Rules "reflect[ed] technology's growing importance to the delivery of legal and law-related services."\textsuperscript{27}

The 2012 amendment to Model Rule 1.1 precludes a lawyer from pleading ignorance of the risks associated with technology. Lawyers are expected to have at least a basic understanding of the risks associated with the technologies they use and the protections available to mitigate those risks.\textsuperscript{28} This obviously includes mobile devices used by lawyers.

The obligation to be aware of the "benefits and risks" of relevant technology under Model Rule 1.1 is a nebulous one, but the Chief Reporter of the ABA Commission on Ethics 20/20 explained that the standard had to be because "a competent lawyer's skill set needs to evolve along with technology itself," and "the specific skills lawyers will need in the decades ahead are difficult to imagine."\textsuperscript{29} Indeed, the risks to client information and how that information should be protected a decade from now will likely be far different than at present.

While attorneys need not become technology experts or "develop a mastery of the security features and deficiencies" of every available technology:

\begin{flushright}
\textsuperscript{25} MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. [8] (amended 2012).
\textsuperscript{26} See, e.g., Fla. Bar, Opinion 10-2 (2010) ("A lawyer who chooses to use [d]evices that contain [s]torage [m]edia such as printers, copiers, scanners, and facsimile machines must take reasonable steps to ensure that client confidentiality is maintained and that the [d]evice is sanitized before disposition.") That opinion explains the obligation to take reasonable steps includes identifying potential threats to client confidentiality involving those devices, implementing policies to address those threats, inventoring devices that contain hard drives or other storage media, and supervising non-lawyers to obtain adequate assurances that confidentiality will be maintained.
\textsuperscript{27} Andrew Perlman, The Twenty-First Century Lawyer's Evolving Ethical Duty of Competence, 22 PROF. LAW., 24, 25 (2014).
\textsuperscript{29} Perlman, supra note 27, at 25.
\end{flushright}
[T]he duties of confidentiality and competence … 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.30

Another proposed state ethics opinion explains that a lack of technical knowledge can render even a highly experienced attorney ethically incompetent to handle a matter "absent curative assistance."31

If an attorney lacks a basic understanding of the risks inherent in the technologies he or she uses to provide legal services, how can the attorney take "reasonable steps" to competently guard against those risks? The duty of competence is the foundation on which the ethical obligation to protect client information rests. As with other skills or practice areas, a lawyer’s duty of technological competence can be achieved through continuing study and education or through association with others who are competent in the area.32

The duty of competence also requires that lawyers be aware of the benefits and risks of emerging technologies that can be used to deliver legal services and how advances in existing technologies can impact the security of information in their possession.33 The difficulty that we face on this issue is the speed at which technology


32 MODEL RULES OF PROF’L CONDUCT R. 1.1 cmts. [2],[8] (2013); Cal. State Bar, Formal Op. 2012-184 (2012) ("If Attorney lacks the necessary competence to assess the security of the technology, she must seek additional information, or consult with someone who possesses the necessary knowledge, such as an information technology consultant."); Iowa State Bar Ass’n, Ethics Op. 11-01 (2011) (noting lawyers can meet due diligence technology requirements "by relying on the … services of independent companies, bar associations or other similar organizations or through its own qualified employees").

is advancing. The mobile phones now carried by many lawyers have more computing power and storage capacity than many desktop computers had a decade ago. When it comes to understanding the risks and benefits of technology, the lawyer's duty of competence must evolve as the technologies we use to provide legal services evolve.\textsuperscript{34}

**IV. THE RISKS ASSOCIATED WITH MOBILE DEVICES**

Mobile devices present several unique risks, which Model Rule 1.1 requires lawyers be aware. The nature of mobile devices "places them at higher exposure to threats" than desktop or laptop computers within a law firm's network.\textsuperscript{35}

While laptop computers present the same type of mobility risks as smart phones, tablets and other portable devices, "the security controls available for laptops today are quite different than those available for smart phones, tablets, and other mobile device types."\textsuperscript{36} Additionally, in many instances laptop computers are owned and supplied by law firms. Therefore, they are excluded from the following discussion of BYOD risk. Law firms can and should exercise complete control over the configuration and security of their laptop computers by removing the user's administrative rights over their laptops and firm-supplied technology equipment. Firms should address in their technology policies the use of technical safeguards such as hard drive encryption, locking down the browser, the use of strong passwords, remote wiping, blocking access to blacklisted web sites and other safety measures for their laptop computers.

Flash drives and external hard drives similarly permit lawyers to transport client and firm information with them, and thus, share the same type of portability risk as mobile devices. But portable flash drives and external hard drives lack the computational and WiFi capabilities of mobile devices. Therefore, they are also excluded from the following discussion of BYOD risks. A law firm should nonetheless consider addressing the portability risk of flash drives and external hard drives in its technology policies. Encrypting flash drives and portable external hard drives or other forms of mobile storage should be considered. And because mobile devices can be

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{34} Cal. State Bar, Formal Op. 2012-184 (2012) (noting "$[a]s technologies change, … security standards also may change" and explaining attorneys "$should keep abreast of the most current standards so that [they] can evaluate whether the measures taken … to protect client confidentiality have not become outdated").
\item \textsuperscript{35} MURUGIAH SOUPAYA & KAREN SCARFONE, NAT'L INST. STANDARDS & TECH., SPEC. PUB. 800-124 REV. 1, GUIDELINES FOR MANAGING THE SECURITY OF MOBILE DEVICES IN THE ENTERPRISE 3 (2013).
\item \textsuperscript{36} \textit{Id}. at 2.
\end{itemize}
\end{footnotesize}
backed up through the use of an external hard drive or a home computer, limiting or prohibiting the transfer of firm or client information to home computers or external hard drives is another issue to consider in the firm's mobile device policy if it is not covered in another firm technology policy.

**Lost or Stolen Device Risk:** The mobility of smart phones and tablets is what makes them so popular; they allow lawyers to potentially transport confidential client and firm information with them or access that information from any place where they can find an internet connection. Given their size and mobility, however, mobile devices can be easily lost, misplaced or stolen. Information that is either stored on or can be accessed by a mobile device may be compromised when a device is lost or stolen.

Last year, it was estimated that 3.1 million smart phones were stolen in the United States and another 1.4 million phones were lost and never recovered. All too often, these devices are protected by weak passwords, or a four-digit PIN that can be "cracked" by a cyber-criminal's brute force attack on the device. A poorly secured mobile device can result in the loss of confidential client or firm information and trigger another risk stemming from a statutory or ethical obligation to report a security incident or data breach to a client or third parties whose information was placed at risk.

**Data Breach Reporting Risk:** Should a mobile device be lost or stolen, a firm must analyze whether the loss triggers a statutory or ethical reporting obligation. This in turn depends on how the device was protected.

The focus of most state data breach notification laws is the unauthorized acquisition or access to unencrypted computerized data that contains personally identifying information. HIPAA is potentially applicable to law firms that qualify as a


40 Forty-seven (47) states, the District of Columbia, the Virgin Islands, Puerto Rico and Guam have adopted data breach notification laws that potentially apply to data breaches involving lawyers and law firms. *See Security Breach Notification Laws, NAT’L CONF. ST. LEG. (Jan. 12, 2015)*,
business associate. The failure to encrypt a mobile device can trigger a duty to report under one or more of the state data breach laws or HIPAA when an inadequately protected mobile device is lost or stolen. In addition to these statutory reporting obligations involving personally identifying or protected health information, a law firm may also have to evaluate whether an ethical duty to report is triggered under Model Rule 1.4 when other types of client information have been compromised as a result of a lost or stolen mobile device.

**Risk That Some Devices Should Not Be Trusted:** While the configuration of smart phones includes basic built-in restrictions or architecture, those security restrictions can be easily compromised by a user in order to download software or third-party applications that would not normally be permitted by the device. This is referred to as jailbreaking (iOS, Apple's operating system) or rooting (Android) a phone, which will provide the user with escalated privileges or root access to the device. Jailbreaking or rooting a smartphone renders it more vulnerable to a malicious attack and should not be permitted in a BYOD environment.41

Some mobile devices are built on platforms that may have vulnerabilities that can be exploited. For instance, it was recently discovered that nearly half of all Android devices are vulnerable "to a newly discovered hack" that allows "attackers to surreptitiously modify or replace seemingly benign apps with malicious ones that steal passwords and other sensitive data."42

Additionally, unless the firm's network has a device directory that recognizes mobile devices that are permitted access, nothing prevents an attorney from using a family member's tablet or smart phone, and gaining access to the firm's network through his or her log-in and password credentials. In this scenario, the lawyer can download client information to the device which will place it completely outside the firm's network and on a device that may lack the protection required by the firm's mobile device policy. This risk can be addressed through technical network or MDM controls that limit access to only mobile devices recognized by the system or data loss

http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Currently, only Alabama, New Mexico and South Dakota have not enacted a data breach notification law. Id.


12
prevention tools that will block the downloading of information to an unrecognized device and through the firm's mobile device policy that prohibits this type of activity.

**Cloud Computing and Shadow IT Risk:** Owners of BYOD devices frequently will download software they prefer to use when working remotely and applications for their personal use during off hours. Thus, BYOD inevitably brings with it BYOS ("Bring Your Own Software") and BYOA ("Bring Your Own Applications") because of their popularity and ease of use. Frequently, this software is cloud based, which means BYOD often also frequently results in BYOC ("Bring Your Own Cloud"). Technology security experts refer to this as the rise of "Shadow IT." Shadow IT refers to IT "solutions used within an [organization] without the approval, or even the knowledge, of corporate IT." It is also "often referred to as the [consumerization] of IT." Vawns Guest & Patrick Bolger, *Managing Shadow IT*, COMPUTERWEEKLY, http://www.computerweekly.com/opinion/Managing-shadow-IT (last visited Apr. 7, 2015).

BYOS, BYOA and BYOC raise additional ethical issues and risks for law firms and their lawyers described below that should be addressed in a firm's technology policies and BYOD policy.

**Insecure Network Risk:** Public WiFi is convenient and easy to use when outside the office, but using it is rife with security risks. When a lawyer connects to public WiFi without the need for a password, the attorney is using an unencrypted connection to an insecure network. The lawyer is vulnerable to eavesdropping and "man-in-the-middle" ("MTM") attacks in this context. A MTM attack redirects a victim's email to the hacker's device, which allows the hacker to compromise the victim's mobile device and can provide the attacker "with access to the corporate network." This risk is one that can be addressed in training sessions and law firm technology policies. Lawyers should be advised to avoid using Public WiFi to work on client documents or to email client or firm information and to turn off any feature on their device that allows it to automatically connect to nearby available networks.

It is unrealistic, however, for a law firm to expect its lawyers will never use an insecure Wi-Fi network when outside the office. Firms should therefore attempt to offer reasonable alternatives for their lawyers that will mitigate this risk. The key to limiting this risk is to provide an encrypted and secure link for communicating and connecting with the firm's network, such as through the use of Citrix or VPN. Law firms should also consider some form of dual factor authentication for remote access to the firm's network.

43 Shadow IT refers to IT "solutions used within an [organization] without the approval, or even the knowledge, of corporate IT." It is also "often referred to as the [consumerization] of IT." Vawns Guest & Patrick Bolger, *Managing Shadow IT*, COMPUTERWEEKLY, http://www.computerweekly.com/opinion/Managing-shadow-IT (last visited Apr. 7, 2015).

**Ediscovery/Spoliation Risk:** A duty to preserve potentially relevant information is triggered when litigation is reasonably anticipated. When a law firm is sued or threatened with a lawsuit, it must preserve electronically stored information ("ESI") in its possession, custody or under its control. This can include ESI stored on attorney or employee-owned mobile devices. Additionally, information on a mobile device may have to be produced in response to a subpoena or reviewed in connection with a government regulation. A law firm's failure to preserve ESI on its lawyer's mobile devices can potentially trigger a spoliation claim. 45

While emails sent or received from a mobile device that is linked to a law firm's email system should be stored on the firm's email server once the device is properly configured and synchronized, text messages and emails sent via a personal, web-based email account on the device will not reside on the firm's servers. And documents potentially can be moved to a Cloud, to a home computer or to a personal storage device from a mobile device. In formulating a litigation hold, law firms should not overlook their employees' mobile devices, home computers and personal storage devices where potentially relevant ESI may be located. It should be anticipated that lawyers will want to protect their personal privacy and limit access to their home computers and personal devices. This can be accomplished by them not transferring work-related ESI to home computers or backing up their devices to home computers or personal storage devices. To limit this clash of interests and to limit the risk of spoliation, a law firm should consider addressing these issues in either its technology policies or specifically in its BYOD policy.

**Privacy Risk:** In *Riley v. California*, the Supreme Court recognized that the owner of a cell phone has a reasonable expectation of privacy in the digital content stored on the phone for purposes of the Fourth Amendment. 46 While the Fourth Amendment is inapplicable to law firms, the Electronic Communications Privacy Act ("ECPA") does apply. The ECPA was intended to protect against privacy intrusions not encompassed by the Fourth Amendment. 47

---

45 See, e.g., Southeastern Mechanical Servs., Inc. v. Brody, 657 F. Supp. 2d 1293 (M.D. Fla. 2009) (awarding spoliation sanctions, in the form of an adverse inference instruction, for failing to properly preserve ESI on BlackBerries). In *Southeastern Mechanical*, BlackBerries were wiped which resulted in the loss of emails before the smart phones were synchronized with the company's email server, as well as the loss of text messages and call logs that would only reside on the device and not the company's servers.

46 134 S.Ct. 2473 (2014) (rejecting the search incident to arrest exception to the Fourth Amendment's warrant requirement).

47 Garcia v. City of Laredo, Tex., 702 F.3d 788, 791 (5th Cir. 2012).
The ECPA protects the privacy of electronic communications, but recognizes an exception that allows the access or interception of electronic communications where consent is provided. The Computer Fraud and Abuse Act ("CFAA") similarly prohibits the unauthorized access to a computer and provides a civil remedy when the damages resulting from that access exceed $5,000.

Law firms generally have a policy on the use of the firm's equipment, computers, email system and network, which explains that the firm monitors the use of these resources and provides that a user should have no expectation of privacy in their use. Some firms may have similar statements on electronic banners that appear whenever a person logs onto the firm's network. These statements may provide that by logging on to the system, accessing the firm's network, or by using its equipment, the user consents to the firm's monitoring the use of the firm's equipment and systems, as well as the firm's review of any documents created or any electronic communications sent or received over its network or via its systems. Similar statements should be included in the firm's BYOD policy to avoid a claim that the ECPA or the CFAA were violated by the firm monitoring work-related emails sent from a personally-owned mobile device.

While these "no expectation of privacy" policies have been generally upheld, one state Supreme Court has ruled to the contrary. In Stengart v. Loving Care Agency, Inc., the New Jersey Supreme Court addressed whether an employer could review emails sent on a company-issued laptop through a personal, password-protected, web-based (Yahoo) email account. The court in Stengart concluded the emails were privileged and observed: "a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications . . . would not be enforceable." While other states have not

---

53 Id. at 665. The court in also noted, however: "Our conclusion that Stengart had an expectation of privacy in e-mails with her lawyer does not mean that employers cannot monitor or regulate the use of workplace computers. Companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy."
followed Stengart's approach, some courts still recognize a privacy distinction between personal and business email accounts and may also consider an employee's efforts to protect documents or emails from review and disclosure even though they are sent from a company computer.

The Stored Communications Act ("SCA") further prohibits the unauthorized access to stored communications, such as email, held by a service provider. The SCA also can be violated when a party "intentionally exceeds" its authorization to gain access to an electronic communication "while it is in electronic storage." When firm or client information is stored in the Cloud by an attorney, the law firm will need the lawyer's permission to delete or remove it from the Cloud to avoid running afoul of the SCA. Firms should consider including an employee consent provision in their mobile device policy which authorizes the firm to remove any client or firm information from a non-approved Cloud that was moved to the Cloud by one of its attorneys.

Should it become necessary to wipe a lost or stolen mobile device, the firm should obtain the lawyer or employee's written permission to avoid a claim under the Computer Fraud and Abuse Act. Both personal and work related information will likely be deleted when the device is wiped. That factor should be spelled out in the law firm's BYOD policy to avoid a claim that the owner of the device did not know the personal

55 In re Info. Mgmt. Servs., Inc. Derivative Litig., 81 A.3d 278, 285 n.1 (Del. Ch. 2013) (explaining that "[a] work email account differs from a personal, password-protected, web-based email account, also known as webmail, which the employee may obtain through Google, Hotmail, or other services" and observing that "[c]ourts have generally afforded greater privacy protection to webmail and have reached divergent conclusions when analyzing the attorney-client privilege if the employee and personal attorney communicated using webmail").
56 See, e.g., Rajaee v. Design Tech Homes, Ltd., Civil Action No. H-13-2517, 2014 WL 5878477, at *3-4 (S.D.Tex. Nov. 11, 2014) (ruling the CFAA was not violated because plaintiff failed to establish that his damages met the Act’s $5,000 threshold following the deletion of personal information on plaintiff's personally owned mobile device by his former employer).
57 See, e.g., People v. Jiang, 33 Cal. Rptr. 184 (Cal. Ct. App. 2005) (holding an employee's emails to his attorney were privileged notwithstanding they were sent via his employer's computer in light of the employee's "substantive efforts to protect the documents from disclosure by password-protecting them and segregating them in a clearly marked and designated folder"). The court in Jiang, however, also noted that the employer's electronic communications policy did not specifically prohibit the employee's personal use of the company's computer system.
59 Id. at § 2701(a)(2).
information would be deleted when the device was wiped and that had he or she known, would not have allowed the device to be wiped.60

Malware Risk: Malware targeting mobile devices has risen significantly and is becoming more complex.61 Depending on the configuration of a law firm's network, these devices may lack the same endpoint security that is available within the firm's firewall for its desktop or laptop computers.62 Antivirus and anti-malware tools require frequent updates to remain effective, which may not be a priority for the device's owner. A compromised smart phone or tablet, however, can serve as a launching pad for malware to steal information from the lawyer who owns the device and to gain a foothold in the law firm's network.

Untrusted Applications Risk: Because a BYOD device is personally owned, a law firm loses control over what applications are downloaded on the device, or what steps the owner takes while downloading any application on the device.63 Many seemingly harmless applications contain security vulnerabilities or malicious payloads that can readily compromise the device.64 A report from Webroot revealed that 42% of

62 Craig Sprosts, Companies Weigh BYOD vs. COPE, But What Really Protects Data?, WIRED, http://www.wired.com/2013/05/companies-weigh-byod-vs-cope-but-what-really-protects-data/ (noting "although there is a litany of anti-virus applications available on the iPhone App Store and in the Android Marketplace, these applications detect a fraction of threats and can be disabled by malware that gains administrative access to the device") (last visited Apr. 8, 2015).
63 TREND MICRO, supra note 61 ("Malware creators are banking on the average user's lack of awareness when it comes to properly setting mobile devices and downloading apps from known safe, legitimate services.").
64 Yulong Zhang, Hui Xue, Tao Wei & Zhaofeng Chen, Freak Out on Mobile, FIREEYE BLOG (Mar. 17, 2015), https:// www.fireeye.com/blog/threat-research/2015/03/freak_out_on_mobile.html ("After scanning 10,985 popular Google Play Android apps with more than 1 million downloads each, we found 1228 (11.2%) of them are vulnerable to a FREAK attack because they use a vulnerable OpenSSL library to connect to vulnerable HTTPS servers. These 1228 apps have been downloaded over 6.3 billion times. Of these 1228 Android apps, 664 use Android's bundled OpenSSL library and 564 have their own compiled OpenSSL library. All these Open SSL versions are vulnerable to FREAK. On the iOS side [Apple iPhones], 771 out of 14,079 (5.5%) popular iOS apps connect to vulnerable HTTPS servers. These apps are vulnerable to FREAK attacks on iOS versions lower than 8.2. Seven [sic] these 771 apps have their own vulnerable versions of OpenSSL and they remain vulnerable on iOS 8.2.").
all Android apps they tested between 2011 and 2013 were classified as malicious, unwanted or suspicious.\textsuperscript{65} With personally owned devices, a firm may also lose the ability to block the user from visiting suspicious websites or URLs that deliver some form of malware to their visitors.

**Unauthorized User Risk:** Another risk involves the unauthorized use of a mobile device by friends, acquaintances and family members that may have access to the device. It is not unusual for a mobile device to be left unattended at home. Applications can be downloaded on the device by family members, and confidential personal information or client information can be accessed if use of the device is not carefully monitored and controlled, even at home.

**Risk of Inappropriate Use:** While law firms may not be able to control how their attorneys use a personally owned mobile device, firms should consider adopting policies and providing training that may help to mitigate that risk. Certain web sites may download malware onto a mobile device when the lawyer visits such a site while surfing the net. This is referred to as a "drive-by-download of malware.” Lawyers should be alerted to this risk and to avoid visiting music, video and adult web sites because of this risk. Another hacker trick is to add a malicious payload into advertisements appearing on sites that appear to be harmless and are frequently visited. When someone clicks on the ad, the payload is launched. Lawyers and staff should be alerted to this risk as well and be advised that they can reduce this risk by either disabling the Java plug-in in the device’s browser or updating the plug-in to its latest version.\textsuperscript{66} And as explained below, a robust MDM application can be potentially


\textsuperscript{66} Java is a programming language that works across multiple computing platforms and is routinely found in plug-ins in web browsers. Java has a history of vulnerabilities. According to Kaspersky Lab, Java was responsible for fifty percent of all cyber-attacks in 2012. See “Oracle Java surpasses Adobe Reader as the most frequently exploited software,” KASPERSKY LAB (Dec. 21, 2012), http://www.kaspersky.com/about/news/virus/2012/Oracle_Java_surpasses_Adobe_Reader_as_the_most_frequently_exploited_software. Symantec has also indicated that hackers continue to “exploit Java vulnerabilities where users have not upgraded to newer, more secure Java versions.” SYMANTEC CORP., INTERNET SECURITY THREAT REPORT 59 (2014), available at http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf.
configured to block access to various web sites and URLs using publicly available blocklists or reputation services.

The risk of distracted driving is well known, and lawyers who attempt to review or send email or text messages while driving place themselves and others at risk. A firm should consider prohibiting the use of a mobile device to review or send email or text messages while driving in either its technology policies or in its mobile device policy. Additionally, law firms should be aware of a recent appellate decision from New Jersey, *Kubert v. Best*, which suggested that a person who sends an email or text message to someone he or she knows is driving a vehicle could be held liable if the driver is involved in an accident while reviewing the message.67 In light of *Kubert*, law firms may want to consider whether it should prohibit sending email or text messages to someone its lawyers or staff know or have reason to know is operating a motor vehicle.

A firm should also clearly provide that its policies prohibiting harassment and discrimination apply to any inappropriate email, text message, blog or social media post sent via mobile device linked to the firm's network. Merely because an inappropriate message or post was sent outside the office during an off-hour will not insulate the firm from potential liability. This is especially true where the firm has advised its employees that they have no expectation of privacy in the use of the firm's network, or systems, and reserves the right to review any emails or communications via devices linked to its network.

**Geo Location Risk:** Mobile devices frequently come equipped with global positioning technology which allows a device to map a location and identify nearby business. These "location services" are frequently used in social media activities and by various applications download on the device which commonly share the user's location with retailers and merchants. Besides compromising the user's personal privacy, location services increase the "risk of targeted attacks because it is easier for potential attackers to determine where the user and the mobile device are, and to correlate that information with other sources" such as "who the user associates with and the kinds of activities they perform in particular locations."68

**Voice to Text Risk:** Many smart phones also have a voice-to-text feature that allows the user to dictate email or text messages sent via the device. While this feature is easy, convenient and more efficient than using your thumbs to type the message, the


68 SOUPAYA & SCARFONNE, supra note 35 at 6.
information dictated to your phone is recorded by the device and sent to third parties for review for quality control purposes.\textsuperscript{69}

**MDM Risks:** Mobile device management (MDM) solutions are available that will segregate personal and firm information on the device, provide a secure connection to a law firm's network and email system, and can help control some of the risks associated with a BYOD approach to mobile technology. MDM applications can be used to enforce strong passwords, lock the device after a specified number of unsuccessful log-ins or after a period of inactivity, encrypt the device and provide the ability to remotely wipe a lost or stolen mobile device. Some MDM solutions can identify smart phones that have been rooted or jailbroken, and have features that can help secure the device’s browser. MDM tools, however, also have vulnerabilities that can be compromised by hackers. Some of these vulnerabilities "include ignoring authentication, sending login tokens without encryption (and in some cases, configuring those tokens to never expire), which could allow an attacker "to wipe innocent phones" or to "access everything the legit [phone] can: email, shared drives, documents, etc."\textsuperscript{70}

There are multiple MDM options available to law firms. These include third-party applications that can be downloaded onto a device in addition to the MDM capabilities that are built into many devices. When deciding which MDM option to deploy the security of these options themselves is a factor to consider, in addition to the types of controls available through each option.

**Wage and Hour/Expense Reimbursement Risk:** Although attorneys are generally considered exempt employees for purposes of wage and hour claims, most law firm employees or staff and paralegals are not exempt and have a right to claim overtime for their off-the-clock work. The Fair Labor Standards Act ("FLSA") mandates that nonexempt employees be paid for work that they are "permitted" to perform.\textsuperscript{71} Additionally, if a law firm "knows or has reason to believe" that work is being performed by nonexempt employees, then it "must count the time as hours worked."\textsuperscript{72} Thus, answering emails or working via mobile devices by nonexempt employees of a

---


\textsuperscript{71} 29 U.S.C. §§203(g) (2014), 207(a) (2010); 29 C.F.R. § 785.11 (2013) ("Work not requested but suffered or permitted to perform is work time.").

\textsuperscript{72} 29 C.F.R. §785.12 (2013).
law firm can potentially trigger a wage and hour claim by those employees unless they are told to keep track of their time and compensation.

Therefore, a law firm should evaluate whether any of its nonexempt employees should be granted access to the firm's network or email system under its BYOD policy. The safest approach to limit or avoid this risk is to exclude nonexempt employees from a firm's BYOD policy and not allow them access to the firm's network or their work-related emails outside of their normal working hours. Should a law firm allow nonexempt employees to access its network or email system under a BYOD policy, to limit this risk the firm should clearly prohibit in writing the use of mobile devices by nonexempt employees for any business-related purpose outside of normal working hours. Firms taking this approach should ensure that nonexempt employees are properly informed about this type of limitation and firms should be prepared to consistently enforce and discipline its violation. Further, lawyers and other supervising nonexempt employees should be aware of this policy and the consequences of not adhering to it.

A related BYOD issue is whether an employee is entitled to reimbursement of some or all of the costs of using a personally owned mobile device. The FLSA prohibits an employer from requiring an employee to pay expenses necessary for the performance of the employee's work when the cost of those expenses "cuts into the minimum or overtime wages required to be paid" under the Act.\textsuperscript{73}

This issue was highlighted by the recent decision in Cochran v. Schwan's Home Service, where the California Court of Appeals ruled that under section 2802 of the California Labor Code, an employer is obligated to reimburse an employee "for the reasonable expense of the mandatory use of a personal cell phone."\textsuperscript{74} The decision in Cochran was not limited to nonexempt employees. So in California, law firms that do not pay or reimburse an employee's cell phone expense under its BYOD policy are at risk for this type of reimbursement claim.\textsuperscript{75}

\textsuperscript{73} 29 C.F.R. §531.35 (2013).

\textsuperscript{74} Cochran v. Schwan's Home Serv., Inc., 176 Cal. Rptr. 3d 407, 412 (Cal. Ct. App. 2014) ("Otherwise, the employer would receive a windfall because it would be passing its operating expenses onto the employee.").

\textsuperscript{75} States that have addressed this issue are not uniform in their approach. Several states have laws similar to California that require employers to reimburse all expenditures necessary or required to perform the employee's work. Other states, however, do not require reimbursement for equipment that may be used for both personal and work related purposes. Still other states follow the FLSA approach and only require reimbursement when the expense would reduce the employee's earnings below minimum wage. So this is a risk that is state specific in nature.
Social Media Risk: Because social media networks such as Facebook, LinkedIn, Twitter, YouTube, Instagram or Snapchat are frequently accessed through mobile devices, any discussion of BYOD risks should include a brief mention of social media risks. Social media users frequently discuss various aspects of their professional and personal lives with their friends and followers in posts or tweets on these networks. One obvious risk is that confidential client or firm information may be inappropriately disclosed in a social media post. Model Rule 1.6 not only encompasses any information relating to the representation of a client, but extends to disclosures "that do not themselves reveal protected information, but could reasonably lead to the discovery of such information by a third person."  

A less obvious social media risk to client information is the role that it plays in spear phishing exploits of hackers and cyber criminals. Hackers scan social media sites looking for information about a target that can be exploited, such as a list of friends, photos or posts about a person's recent activities. Cyber criminals hope that because a phishing email appears to be from someone the intended target knows or recognizes, they will be less careful in handling the email and either click on a link or an attachment containing malware, or provide information in response to the email that they would not otherwise provide to a stranger.

There is no magic bullet to defeat these exploits. The best way to prevent a successful spear phishing attack is through ongoing training to all lawyers and staff about to how to identify phishing emails and social engineering tricks coupled with frequent reminders to never click on attachments or links in suspicious emails or in emails from someone they don't know or emails they were not expecting to receive.

V. THE ETHICAL DUTY TO SAFEGUARD AGAINST TECHNOLOGY-BASED RISKS

If the foundation of a lawyer's ethical duty to safeguard client information is found in Rule 1.1, then Model Rules 1.6 and 1.15 provide the ethical "firewall" that protects client and firm information from the "barbarians" who are seeking access at the "castle's gates."

Model Rule 1.15 requires a lawyer to "hold property of clients or third persons" in the lawyer's possession "separate from the lawyer's own property," and mandates

77 Spear phishing involves a phony or spoofed email that appears to be from a person, company or organization that the intended target knows. Successful spear phishing exploits rely on familiarity with the intended target.
that it be "appropriately safeguarded."\(^\text{78}\) Comment 1 to Rule 1.15 explains, "[a] lawyer should hold property of others with the care required of a professional fiduciary."\(^\text{79}\)

Rule 1.15 applies to property of clients and third persons irrespective of its format; it applies with equal force to tangible property, paper records and electronic information.\(^\text{80}\) Comment 1 to Model Rule 1.15 explains it also applies to property received from "prospective" clients.\(^\text{81}\)

As it pertains to data security, Rule 1.6 states that a lawyer "shall not reveal" any information "relating to the representation of a client unless the client gives informed consent, [or] the disclosure is impliedly authorized . . . to carry out the representation."\(^\text{82}\) Rule 1.6 is not limited to information protected by the attorney-client privilege but "to all information relating to the representation, whatever its source."\(^\text{83}\) It extends to disclosures "that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person."\(^\text{84}\)

Lawyers are obligated to take "reasonable measures" to safeguard "the integrity and security" of their electronic files.\(^\text{85}\) Among other things, this obligation requires that lawyers take "reasonable steps" to ensure that "only authorized individuals have access to the electronic files" and to ensure they "are secure from outside intrusion."\(^\text{86}\) Rule 1.6(c) requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."\(^\text{87}\)

Comment 18 lists a series of factors to consider in assessing whether “reasonable efforts” were taken to protect against an inadvertent or unauthorized disclosure or access of information, including:

\(^{78}\) Model Rules of Prof'L Conduct R. 1.15(a) (2013).


\(^{80}\) See, e.g., Pa. Bar Ass'n, Formal Op. 2011-200 (2011) ("Client property generally includes files, information and documents, including those existing electronically.").


\(^{82}\) Model Rules of Prof'L Conduct R. 1.6(a) (2013).


\(^{86}\) Id. (explaining such steps include the use of firewalls, intrusion detection software and backups of all electronically stored files).

\(^{87}\) Model Rules of Prof'L Conduct R. 1.6(c) (2013).
• The sensitivity of the information.
• The likelihood of disclosure if additional safeguards are not taken.
• The cost of employing additional safeguards.
• The difficulty of implementing the safeguards.
• The extent to which the safeguards adversely affect a lawyer’s ability to represent a client.
• Whether the client required special security measures be taken or provided informed consent to forego security measures that might be required under this rule.88

Thus, Rule 1.6 contemplates a balancing approach when evaluating the security measures that can or should be taken when protecting client information. Various state ethics opinions take a similar approach to the issue.89 Those opinions recognize that "facts and circumstances" can dictate the types of "reasonable protective measures" a lawyer must take to protect information in the lawyer's possession.90 The level of protection may depend on the "type and sensitivity of client information."91 As one ethics opinion explained:

The greater the sensitivity of the information, the less risk an 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.92

89 See, e.g., Cal. State Bar, Formal Op. 2010-179 (2010) (outlining various factors to consider including "the degree of sensitivity of the information").
90 Id.; Iowa State Bar Ass'n, Ethics Op. 11-01 (2011).
91 N. H. Bar Ass'n, Advisory Op. 2012-13/4 (2013) (addressing cloud computing); see also Iowa State Bar Ass'n, Ethics Op. 11-01 (2011) (recognizing "the degree of protection to be afforded client information varies with the client, matter and information involved").
92 Cal. State Bar, Formal Op. 2010-179 (2010); see also Fla. Bar, Op. 12-3 (2013) (addressing cloud issues involving "particularly sensitive information" and noting a "lawyer should consider whether [to] use the outside service provider or use additional security in [these] specific matters").
These opinions suggest that lawyers and law firms should identify various types of “highly” sensitive information in their possession.

While ethics opinions explain that additional precautions should be considered in various contexts when "highly" or "particularly" sensitive information are involved, they generally do not define or discuss the types of client information that would be encompassed by that rubric. It seems logical, however, for law firms to consider addressing the sensitivity of client information at the outset of any engagement.

This can be accomplished in several ways. The client can be asked if the engagement will involve any highly sensitive information or information warranting special security measures. Additionally, the file intake process can be set up to identify any categories of information that state or federal law treat as highly sensitive in nature or that the firm believes should be treated as highly sensitive. Examples could include personally identifying information, protected health information, non-public financial information, proprietary information, source code, patents, trademarks, trade dress, trade secrets, a merger and acquisition or a high stake business deal. A firm can then take any steps it deems necessary and appropriate to protect that information, including limiting who is permitted to access that information and how it may be transmitted.

Rule 1.6 recognizes that additional safeguards may be required with highly sensitive information, while also noting the cost and difficulty of implementing or using certain types of safeguards are relevant considerations when evaluating whether to apply additional safeguards. The additional safeguards, however, do not have to be technology based. They can, and should, include security awareness training and the development of firm policies involving the use of technology by a firm's lawyers and staff.

The ethical duty to take reasonable precautions clearly does not require measures that will "guarantee" against unauthorized access. Rule 1.6's duty of confidentiality “does not require that a lawyer use only infallibly secure methods” to store and transmit information.


Various ethics opinions have referenced a number of technological options available to protect client information.95 Given the speed at which technology is evolving, state ethics opinions generally avoid recommending any particular security measure for fear it will be quickly outmoded.96 Therefore, state ethics opinions generally leave it to the "sound professional judgment" of the attorney to determine what type of security measures should be taken.97

Comment 18 to Rule 1.6 further notes that whether additional steps are required to comply with other laws such as state and federal laws governing data privacy is beyond the scope of the Rule.98 However, HIPAA's Security Rule applies to lawyers and firms that qualify as "business associates" and imposes various physical, administrative and technical safeguards designed to ensure the confidentiality, integrity and access to electronic personal health information.99

Law firms should not overlook training on data security and the development of policies as important data security measures in accordance with Rule 1.6. If there is one truism when it comes to data security, it is that no technological safeguard is foolproof or can entirely eliminate the risk of unauthorized access to client data. Law firms can have advanced technological safeguards built into their email and information systems, but if lawyers do not know how to use the firm's technology, then those safeguards are rendered worthless. As a result, technology and data security training is an important component to any risk management program for law firms.

95 Ariz. State Bar, Ethics Op. 09-04 (2009) ("In satisfying the duty to take reasonable security precautions, lawyers should consider firewalls, password protection schemes, encryption, anti-virus measures, etc.").

96 See, e.g., Iowa State Bar Ass'n, Ethics Op. 11-01 (2011) ("It is beyond the Committee's ability to conduct a detailed information technology analysis .... Even if we had that ability our analysis would soon be outdated.").

97 Ariz. State Bar, Ethics Op. 05-04 (2005) ("Precisely which of these software and hardware systems should be chosen – and the extent to which they must be employed – is beyond the scope and competence of the Committee. This is the kind of thing each attorney must assess."); N. J. Sup. Ct., Op. 701 (2006) (explaining a lawyer "is required to exercise sound professional judgment on the steps necessary to secure client confidences against foreseeable attempts at unauthorized access"); Mass. Bar Ass'n, Ethics Op. 12-03 (2012) ("Ultimately, the question of whether the use of Google docs, or any other Internet based data storage service provider, is compatible with [a] Lawyer's ethical obligation to protect his clients' confidential information is one that Lawyer must answer for himself based on the criteria set forth in this opinion....").


An attorney's duty of confidentiality and the corresponding duty to take appropriate measures or reasonable steps to protect information in a lawyer's possession do not require an attorney-client relationship to exist before it is triggered, as the duty of confidentiality applies once information is received from "prospective" clients.\textsuperscript{100} Also, Rule 1.6's duty of confidentiality does not end upon the termination of the attorney-client relationship.\textsuperscript{101} Rule 1.9(c) extends the duty of confidentiality to "former clients" and provides: "A lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client . . . shall not thereafter . . . (2) reveal information relating to the representation except as these Rules would permit or require with respect to a client."\textsuperscript{102}

Options to protect information stored on a mobile device and comply with the duty of confidentiality could include:

- Protecting it with a strong password.
- Encrypting the device.
- Installing and frequently updating antivirus/anti-malware protection on device;
- Investigating the reputation and reviews of any application before downloading the application on the device,
- Refusing to open attachments or click on links or photographs in any email from an unknown person or in a suspicious looking email you were not expecting to receive;
- Avoiding clicking on advertisements when visiting websites and avoiding websites that have been publicly blacklisted by reputation services;
- Training lawyers and staff on risks and best practices for mobile device use and security.
- Employing a combination of some or all of the above steps.

\footnotesize
\textsuperscript{100} See Model Rules of Prof'l Conduct R. 1.18(b) (2013) (addressing information received from "prospective" clients and explaining "[e]ven when no client-lawyer relationship ensues, a lawyer … shall not use or reveal that information, except as Rule 1.9 would permit").


\textsuperscript{102} Model Rules of Prof'l Conduct R. 1.9(c) (2013).
The types of physical, administrative and technical safeguards a firm may want to consider when adopting a BYOD approach to mobile technology to safeguard client and Firm information are outlined below in Part VI.

VI. DUTY TO HAVE MEASURES REASONABLY ASSURING THAT LAWYERS ARE CONFORMING TO PROFESSIONAL CONDUCT RULES AND THE CONDUCT OF NON-LAWYER ASSISTANTS IS COMPATIBLE WITH LAWYERS PROFESSIONAL OBLIGATIONS

Most lawyers do not have an IT background or training in computer or network security. That means that law firms must rely on the assistance of IT professionals to create a network infrastructure that will allow its lawyers to work remotely and communicate electronically. This reality triggers the application of Rules 5.1 and 5.3 of the Model Rules of Professional Conduct.

Rule 5.1 imposes supervisory obligations on partners or lawyers with "comparable managerial authority" to ensure the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.103 This requires "reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance" that the firm's lawyers will conform to the Rules of Professional Conduct including the duty of competence in Rule 1.1 and the duty of confidentiality in Rule 1.6.104

Some lawyers value convenience over security and may deliberately work around a firm’s security measures because they either fail to appreciate the risk of their conduct or simply do not care. A law firm’s most tech-savvy lawyers, its Millennials, are the ones most likely to try to circumvent its security rules.105 While training can help explain the risk to client data, a law firm should consider data security policies that prohibit risky conduct. A law firm must consistently enforce its data security policies and practices in order for them to be effective. This is especially true with personally owned mobile devices.

The development of policies and practices addressing data security, the appropriate use of firm equipment, maintaining the confidentiality of client information, safe internet practices, and associated training on these topics are examples of efforts that can provide "reasonable assurance" that the firm's lawyers are complying with their ethical duties involving data security. Part VI of this article contains

103  MODEL RULES OF PROF'L CONDUCT R. 5.1(a) (2013).
recommendations for Firms to consider when developing a BYOD policy relating to mobile device technology. Whether additional measures beyond "internal policies and procedures" are required will depend on the firm's size and structure, the experience of its lawyers, the nature of its practice and the frequency with which difficult ethical issues arise.106

Rule 5.3 takes an identical approach with non-lawyers who are employed, retained or associated with a lawyer or firm. It requires partners and any lawyer or group of lawyers with "comparable managerial authority" to ensure that the firm has in effect measures giving reasonable assurance that the conduct of non-lawyer assistance "is compatible with the professional obligations of the lawyer."107 This means that non-lawyers who work within the firm (e.g., secretaries, IT specialists, docket clerks, paralegals) and those who work outside the firm (e.g., court reporters, IT consultants, expert witnesses, ediscovery vendors) should understand the need to preserve the confidentiality of client and firm information to which they have access.

Comment [2] to Model Rule 5.3 explains that non-lawyer assistants must be given "appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product."108 The same is true for non-lawyer assistants who work outside the firm. The extent of this obligation turns on several factors including: the education, experience and reputation of the non-lawyer assistant; the nature of the services provided by the assistant; the terms of any arrangements relating to the protection of client information; as well as the "legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality."109 Law firms should not overlook training for its employees and staff on data and cyber security and the confidentiality obligations imposed on the firm and its lawyers.

A. Cloud Computing and Cloud Storage Ethical Issues Arising From Mobile Technology

The term cloud computing refers to the shared use of applications, computing services, and physical or virtual resources over the internet.110 Examples of cloud computing applications (BYOA or BYOS) available to lawyers and law firms include

107 Model Rules of Prof'l Conduct R. 5.3(a) (2013).
Google Docs, Carbonite, SugarSync, Dropbox and Microsoft Office 365. Documents generated or shared through web-based applications like these are generally stored in the "cloud." Web or internet based email systems such as Gmail and Yahoo also store email and attachments in the "cloud."

Cloud storage refers to an internet-based model of remote data storage on servers typically owned by third parties that host the data, generally at off-site locations. Cloud storage is simply today's version of a warehouse for electronic records. References to the "cloud" are merely "a fancy way of saying stuff's not on your computer."

There are three basic delivery models for cloud computing services. Software as a service (SaaS) is the name of a model though which applications are made available to a user through an interface with the user's computer. Platform as a service (PaaS) is a model used primarily to develop those applications. Infrastructure as a service (IaaS) typically involves a third party host that provides computing resources, such as hardware, servers, storage and other components of a network's infrastructure. Lawyers and law firms would be generally involved with SaaS and IaaS cloud delivery models.

Cloud computing resources are made available or deployed in one of four ways:

- Public clouds which are available for use over a public network by anyone;
- Private clouds which are available for use solely by the employee of a single organization;
- Community clouds which are available to organizations or entities within the same or related service industries or community; or
- Hybrid clouds, which can involve a combination of a public cloud provider with a private cloud platform to perform distinct functions for a single organization. A hybrid cloud provides an organization the flexibility to store information in a private cloud while relying on applications and other computing resources from a public cloud to create or transmit information.

Cloud applications and cloud-based storage typically go hand-in-hand with today's mobile devices by virtue of applications and web based email accounts on those devices. Cloud-based applications and mobile technology permit lawyers greater flexibility in how they can access and share documents, information or work. Documents or emails can be accessed wherever, whenever and however network or WiFi access can be obtained. Cloud applications and storage can provide significant cost savings to lawyers and firms by eliminating the need to purchase, maintain, upgrade and patch hardware, servers and software applications on an on-going basis; to employ staff to perform those functions; or to rent space to house that equipment. And the security measures that reputable, certified cloud storage providers have in place likely exceed the security of most law firms.113

The use of the cloud, however, implicates the lawyer’s duty of competence under Rule 1.1.114 Because use of the cloud means that client information will be stored on a third party’s servers, it poses a different set of security risks, as third parties may be permitted to have some form of access to client information. A lawyer's duty to safeguard information under its control cannot be transferred or delegated to a third party, nor is it lessened simply because the lawyer stores client information with a cloud provider.115 Thus, mobile technology's use of the cloud also triggers consideration of Model Rules 1.6, 1.15, 5.1 and 5.3. Yet how many lawyers have considered whether their use of cloud-based applications or web-based mail accounts on their mobile devices trigger these issues? And how many lawyers have checked Google's terms of service for instance, and evaluated the potential impact of those service terms on the duty to maintain the confidentiality and security of client information?116

113 See, e.g., N.J. Sup. Ct. Op., 701 (2006) (recognizing that "[p]roviding security on the Internet against hacking and other forms of unauthorized use has become a specialized and complex facet of the industry" and "it is not necessarily the case that safeguards against unauthorized disclosure are inherently stronger when a law firm uses its own staff to maintain a server").


116 Google's terms of service, which are available at, http://www.google.com/intl/en/policies/terms/ provides in pertinent part:

When you upload, submit, store, send or receive content to or through our Services, you give 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
At present, twenty (20) states have issued ethics opinions addressing the use of cloud computing or cloud storage. The ABA maintains a list of state ethics opinions. While there are variations in these ethics opinions, they generally permit the use of cloud computing and cloud storage, but require the lawyer to exercise reasonable care in the selection of a cloud vendor and in assessing the vendor's procedures for safeguarding the confidentiality of client information. They require a lawyer to evaluate whether a cloud provider’s terms of use, policies, practices and procedures are compatible with the lawyer’s professional obligations.

New York opinion 842 explains that exercising “reasonable care” in this context “may” include:

• Verifying the cloud storage provider has an enforceable obligation to preserve confidentiality and will notify the lawyer if served with process requiring the production of client information.

• Investigating the adequacy of the cloud provider’s security, policies, recoverability methods, and other procedures.

• Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

• Investigating the cloud provider’s ability to purge any copies of the data, and to move the data to a different host for any reason.

Pennsylvania Formal Opinion 2011-200 suggests several other factors that lawyers should consider, including whether the cloud provider:

better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services ....


See, e.g., N. Y. State Bar Ass'n, Ethics Op. 842 (2010) (concluding that lawyers may ethically use cloud storage so long as they take "reasonable care to ensure that the system is secure and that client confidentiality will be maintained"); Ala. State Bar, Ethics Op. 2010-02 (2010) (determining "a lawyer may use 'cloud computing' or third-party providers to store client data provided that the attorney exercises reasonable care in doing so").


• Explicitly agrees that it has no ownership or security interest in the data.

• Includes in its terms of service or service level agreement an explanation of how confidential client information will be handled.

• Provides a method for retrieving data if the provider goes out of business, the service has a break in continuity or the agreement is terminated.

• Employs technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing.

• Provides the law firm with the right to audit the provider’s security procedures and to obtain copies of any security audits performed.

• Agrees to host the data only within a specified geographic area.\textsuperscript{121}

On this last point, another state ethics opinion addressing a virtual law practice suggests lawyers should:

\begin{quote}
\textquote{[A]ddress and minimize exposure of the client to legal issues triggered by both the international movement, and/or storage, of information in the cloud, and the potential subcontracting out of one vendor’s services to unknown third-party vendors, which may impact confidentiality, without the prior written consent of Attorney and affected clients.}\textsuperscript{122}
\end{quote}

Pennsylvania Opinion 2011-200 further explains that should the data be hosted outside of the United States, then the law firm should determine that “the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States.”\textsuperscript{123} It further suggests that a lawyer investigate the cloud provider’s:

• Security measures, policies and recovery methods.

• System for backing up data.

• Security of its data centers and if storage is provided in multiple centers.

\begin{flushright}
\end{flushright}
• Safeguards against disasters, including multiple server locations.

• History, including the length of time it has been in business, and its funding and stability.

• Process used to comply with data subject to a litigation hold.124

A lawyer's obligation to confirm that a cloud provider can reliably maintain the confidentiality of client information can be satisfied through "compliance with industry standards," provided those standards "meet the minimum requirements imposed on the [l]awyer" by the State Rules of Professional Conduct.125 A lawyer should verify that the cloud provider will either return or securely delete information from the cloud once an engagement ends or there is no longer a need to retain the information and then evaluate the process to be used to accomplish that task.126 "Otherwise, the lawyer's duty to take reasonable steps to protect the security and confidentiality of that data" will continue indefinitely.127

A highly relevant inquiry is whether the cloud provider has ever suffered a security breach, and if so, how the breach (or breaches), occurred and what steps have been taken to prevent a reoccurrence.128

Given the increasing importance of encryption to data security, lawyers should inquire if the cloud provider encrypts information before it is stored in the cloud, if the provider has a process through which client information can be encrypted or if the provider will assist the lawyer to encrypt information before it is stored in the cloud. And if a cloud provider periodically transmits data between servers at remote locations, the lawyer should confirm the data is encrypted while in transit so it remains adequately protected while en route.

---

124 Id.
128 See N. Y. State Bar Ass'n, Ethics Op. 842 (2010) (explaining that if a lawyer learns of a data breach of an "online storage provider," the lawyer must investigate whether the breach involved the client's data, notify any affected clients, "and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated"); see also Alaska Bar Ass'n, Ethics Op. 2014-3 (2014) (noting a "lawyer must notify the impacted client if the lawyer learns that the provider's security was breached and the client's confidence or secret was revealed").
As with any other use of technology, lawyers "should conduct periodic reassessments" of these factors to verify that a cloud vendor's security measures "have not become outdated" in light of changing technology or "that changes in the vendor's business environment or management have not negatively affected [their] adequacy."\(^{129}\)

Finally, law firms should consider rules and policies that prohibit the use of public clouds by attorneys or staff that have not been carefully evaluated and approved by the firm. This would include the use of mobile technology and applications that store sensitive or confidential client information in public clouds without the firm's prior express authorization.

**B. Is Client Consent Required?**

Whether client consent is required for the use of cloud computing appears to be an open question. Several of the ethics opinions that discuss the issue suggest that its use may be “impliedly authorized” under Model Rule 1.6 so long as reasonable efforts are used to ensure the data is adequately safeguarded.\(^{130}\)

In an opinion addressing remote access to client files, the New York State Bar Association took the position that when a law firm is able to make a determination that the security measures in place are reasonable, client consent is unnecessary.\(^{131}\) The use of the cloud, however, is just another form of outsourcing.\(^{132}\) Thus, while ABA Formal Opinion 08-451 does not specifically address use of the cloud, it simply cannot be ignored. Opinion 08-451 takes the position that when an outsourcing relationship is attenuated, client consent is required before information covered by Rule 1.6 is shared.


\(^{130}\) See, e.g., Pa. Bar Ass'n, Formal Op. 2011-200 (2011) ("This may mean that a third party vendor, as with 'cloud computing,' could be 'impliedly authorized' to handle client data provided that the information remains confidential, is kept secure, and any disclosure is confined only to necessary personnel."); N. H. Bar Ass'n, Advisory Op. 2012-13/4 (2013) ("As cloud computing comes into wider use, storing and transmitting information in the cloud may be deemed an impliedly authorized disclosure to the provider, so long as the lawyer takes reasonable steps to ensure that the provider of cloud computing services has adequate safeguards."); Nev. State Bar, Formal Op. 33 (2006) (explaining if the third party electronic storage vendor "can be reasonably relied upon to maintain the confidentiality [of client information] and agrees to do so, then the transmission is permitted by the rules even without client consent").


with "outside" entities or individuals "over whom the firm lacks effective supervision and control."\footnote{ABA, Formal Op. 08-451 (2008).}

One state ethics opinion addressing a virtual law practice that was entirely cloud based explained that the "virtual" attorney:

\[S\text{hould consider whether her ethical obligations require that she make appropriate disclosures and obtain the client's consent to the fact that an outside vendor is providing the technological base of Attorney's law firm, and that, as a result, the outside vendor will be receiving and exclusively storing the client's confidential information.}\footnote{Cal. State Bar, Formal Op. 2012-184 (2012).}

Several other state ethics opinions suggest that client consent may be required when highly sensitive information is involved.\footnote{Cal. State Bar, Formal Op. 2010-179 (2010) ("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.").} New Hampshire, for instance, explains "where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent."\footnote{N.H. Bar Ass'n, Advisory Op. 2012-13/4 (2013).} Ohio State Bar Association's Informal Advisory Opinion 2013-03 appears to echo this view, stating "[i]n exercising judgment about whether to consult with the client about storing client data in ‘the cloud,’ the lawyer should consider, among other things, the sensitivity of the client's data."\footnote{Ohio State Bar Ass'n, Informal Advisory Op. 2013-03 (2013); see also Alaska Bar Ass'n, Ethics Op. 2014-3 (2014) ('Where highly sensitive data are involved, it may behoove a lawyer to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent.').}

The Pennsylvania Bar Association, while not explicitly requiring informed consent, concludes "it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of 'cloud computing' and the advantages as well as the risks endemic to online storage and transmission."\footnote{Pa. Bar Ass'n, Formal Op. 2011-200 (2011)(further explaining that under Rule 1.4, "adequate information' should be provided to the client so that the client understands the nature of the representation and 'material risks' inherent in an attorney's methods").}
Other states' ethics opinions provide more explicit guidance on the issue. Massachusetts Opinion 12-03 addressed the use of Google Docs and concluded that while the use of an internet-based service provider would not violate Rule 1.6 under normal circumstances, a lawyer “remains bound to follow an express instruction from his client that the client's confidential information not be stored or transmitted by means of the Internet, and that he should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so.”\(^{139}\)

One of the difficulties surrounding the issue of client consent is that no two cloud applications or vendors are the same. Cloud vendors employ different procedures and safeguards. Moreover, cloud computing has a myriad of potential uses by a law firm. Obtaining client consent for a specific project, such as an e-discovery review platform in litigation or a file sharing application when collaborating on a transaction, is eminently reasonable and can be easily accomplished.

When, however, a cloud based application or computing resource will be used enterprise-wide on an on-going basis by a lawyer or law firm, obtaining client consent may raise a problematic issue. It is unrealistic, for instance, to expect a law firm to have two email systems, one that is cloud-based and a second for those clients that do not consent to the firm's cloud-based email system. So long as a firm has carefully evaluated the cloud-based application, its security and its procedures for safeguarding the confidentiality of client information, the firm should be ethically permitted to use the application.

In light of the quagmire of ethics opinions surrounding the issue of client consent involving a lawyer's use of the cloud, lawyers should carefully evaluate the issue in the context in which the cloud-based application(s) would be used. Given the various ethics opinions noted above, lawyers should carefully address the issue of client consent where highly sensitive information may be involved. Remember when seeking client consent, a lawyer must disclose the risks of using that technology so that the client's consent is "informed."\(^{140}\)

Lawyers and law firms should consider addressing the use of the cloud in their engagement letters, explaining how they use the cloud and its potential ramifications in terms that clients can understand. Then a client cannot claim he or she did not know about the lawyer's use of the cloud should a breach occur.

**VII. RECOMMENDATIONS FOR LAW FIRMS ADOPTING A BYOD APPROACH TO MOBILE TECHNOLOGY**


Any law firm that has adopted a BYOD approach to mobile technology should consider developing a comprehensive written data security policy addressing the risks presented by its BYOD program. The policy should address the appropriate use of the mobile devices by the firm's employees, and should clearly spell out that access to the firm's network is conditioned upon full and continuing compliance with the firm's data security policy for mobile devices. The policy should provide that the right to access the firm's network will be immediately terminated if the policy is violated and upon the resignation, retirement or termination of the device's owner from the firm. The policy should further provide that its violation can result in discipline up to and including termination from the firm.

In developing a BYOD program, the firm should also give careful consideration to who will be granted access to the firm's network. Options include all employees, only attorneys, only partners or some combination thereof. To the extent that nonexempt employees of the firm are included, a firm may face wage and hour risk outlined in Part IV above.

The firm should also consider what types of mobile devices will be encompassed by its BYOD policy, which may be influenced by other technology policies the firm has adopted. Should laptop computers or tablets be included or just smart phones? Even though home computers and external storage devices obviously fall outside the parameters of a BYOD policy, the firm should consider including a provision in its mobile device policy that prohibits backing up a mobile device or transferring any firm or client information via a mobile device to a home computer or personal storage device.

Once the type of devices to include in the policy has been determined, the firm should next consider the brands or models of those devices it is willing to support. Relevant considerations include the relative security and continuing viability of various device models and their operating systems, as well as the security of applications that are available from an applicable app store.

Another scope issue to consider is what aspects of the firm's network or what types of data or information an employee will be allowed to access from his or her mobile device. Group policies should be applied to all mobile devices linked to the firm's network with a view to allowing access to only those aspects of the network that are necessary for the particular attorney or employee.

Because lost or stolen devices are one of the major causes of data breaches, the firm's policy should prohibit downloading of any client or firm information on the device. The policy should also require the device owner to immediately report when
any mobile device linked to the firm's network is lost or stolen. Otherwise, the firm will be unable to promptly wipe a lost or stolen device.\footnote{The ability to remotely wipe a lost or stolen device should not be viewed as a panacea by the firm or its lawyers. The ability to remotely wipe the device requires that it be turned on and has battery life remaining on the device.}

Given the privacy risks outlined in Part IV, the written consent of the device owner to the firm monitoring use of the device, wiping information from the device and obtaining access to it when necessary is a critical feature of any BYOD policy. The policy should also clearly warn the device owner that should remote wiping of the device become necessary, it will likely result in the loss of all personal information on the device.

The policy should also spell out when access to the device itself may be required, \textit{e.g.}, when imposing a litigation hold, in response to a subpoena or governmental investigation, before the device is sold or possession of it is transferred to a third party, or upon the owner's termination or resignation from the firm. The policy should clearly explain the circumstances which will require or permit the firm to wipe the device, \textit{e.g.}, if the device is lost or stolen, if an employee fails to temporarily make the device available to allow client and firm information to be removed before the device is sold or transferred, or upon the owner's resignation or termination from the firm. The policy should further reserve the right to inspect and monitor the device to confirm continued compliance with the firm's mobile device policy. The policy should also advise owners that they have no expectation of privacy in emails or text messages in any device linked to the firm's network or email or information systems.

The firm should consider addressing various inappropriate uses of mobile devices in its policy. Because devices that have been jailbroken or rooted are particularly susceptible to malware, the firm should consider prohibiting attempts to alter or disable any of the device's built-in security features, and to immediately terminate access to its network when it discovers such a policy violation. The firm's policy should prohibit attempts by its lawyers to gain access to the firm's network or systems by using a third party's device. The firm may also want to state in its policy that it prohibits reviewing or sending email or text messages while operating a motor vehicle. A BYOD policy should provide that the firm's other technology policies, such as those dealing with passwords and acceptable use of technology apply to personally owned mobile devices that are linked to the firm's network. Additionally, the firm's BYOD policy should state that the firm's policies prohibiting harassment and discrimination apply to the use of mobile devices, irrespective of where or when an inappropriate use of a device might occur.
If the firm prohibits the transfer of firm or client information to the cloud, or permits data to be moved to a firm-approved cloud, that policy should be applied to the use of mobile devices and set forth in its mobile device policy. If a firm has not yet considered cloud issues in its technology policies then it should consider addressing the issue in its BYOD policy since it is likely that at least some of the firm's lawyers have a personal, web-based email account and may have downloaded applications on their device that will automatically store communications and documents in the cloud.

Physically safeguarding the device should also be addressed in the firm's mobile device policy. The policy should provide that the device will remain in the owner's possession and prohibit unsupervised access of the device by family, friends or third parties.

Another critical consideration is the technical safeguards that a law firm will require as a condition of accessing its network. Many devices have MDM applications in the device's operating system and third party MDM applications are available that can be downloaded on the device, which provide the firm with a range of options and even greater controls. MDM applications can allow firms to segregate firm and personal data on the device in separate containers, and depending on the application, allow the device to be configured so as to require one or more of the following controls:

- Strong, complex passwords or biometric security for access to the device;
- Encryption of all data stored on the device;
- Separation and segregation of personal emails, contacts, calendars, notes, reminders and call logs from the firm side of the device to maintain the privacy of the owner's information;
- Locking the device after a specified period of inactivity;
- Wiping a lost or stolen mobile device and/or the use of a remote location feature to find a lost device;
- Locking or remotely wiping the device after a certain number of unsuccessful attempts to log onto the device;
- Prohibiting access to the network by devices that are jailbroken or rooted or unrecognized devices;
- Browser policies that will warn or deny access to certain web sites;
- Data loss prevention policies including data backup restrictions;
- Scanning and assigning risk profiles based to apps on the device;
• Providing a secure tunnel or VPN between the firm side of the device and the firm's network.

Any technical controls for mobile devices, like those outlined above, that the firm requires as a condition of gaining access to its network, should be spelled out in its mobile device policy.

Any BYOD program would not be complete without training. A firm's lawyers and staff should be trained on its technology policies and its data security policy for mobile devices. One effective approach to technology training is to personalize the message. No one wants to be the victim of a cyber-crime or have his or her identity stolen. Explain that by following the firm's security requirements, they will be protecting themselves, their families and their loved ones, and in the process will also be protecting their law firm.

Training should not be limited to the firm's mobile device and other technology policies but can explain why strong passwords are important, address phishing schemes, social engineering and other hacker tricks,\textsuperscript{142} signs that a computer or device may be infected with malware or may be hacked and who to contact should they believe that to be true.

Finally a BYOD program is not something that a law firm can roll out with a policy and then ignore. New applications are being developed on a daily basis and new vulnerabilities are being identified almost as quickly. Hackers are omnipresent and developing new attack strategies and modifying malware in an attempt to avoid the latest technological defenses. A firm's mobile device policy should be periodically reviewed and evaluated and improved and refined whenever possible. Indeed, the various ethics opinions discussed above explain that is our ethical obligation.

While a comprehensive BYOD policy, coordinated physical, administrative and technical safeguards and a robust training program are no guarantee against the risk of being hacked, they will certainly mitigate that risk. Remember the watch commander's warning on Hill Street Blues: "Let's be careful out there."

VIII. SAMPLE LAW FIRM BYOD POLICY

[INSERT LAW FIRM NAME]

\textsuperscript{142} The New York City Bar Association recently issued an ethics opinion which expressed the view that an attorney’s “duty of competence includes a duty to exercise reasonable diligence in identifying and avoiding common Internet-based scams.” N.Y. City Bar Ass’n, Formal Op. 2015-3 (2015).
DATA SECURITY POLICY FOR MOBILE DEVICES

The rules governing the legal profession require that lawyers act competently to safeguard information relating to the representation of a client against its inadvertent or unauthorized disclosure and to take reasonable precautions to prevent the unauthorized access of client information. Additionally, HIPAA imposes an obligation to safeguard Protected Health Information (PHI) and various other state and federal statutes require the safeguarding of Personally Identifiable Information (PII). [Some of our clients and insurance carriers are imposing additional security requirements on our Firm.]

Many of the Firm’s lawyers own mobile devices on which email can be sent or received, and information or documents can be accessed, stored or transmitted electronically. While it is not necessary to the performance of legal services, the Firm does allow these personally owned mobile devices to be linked to the Firm’s network, email and information systems as a convenience to our lawyers who may choose to use a mobile device, but are not obligated to do so, when providing legal services to the Firm’s clients. As a result, confidential or proprietary client or Firm information, nonpublic financial information, PHI and PII may reside on these devices or may be transmitted via these devices. The use of these devices can also result in confidential or proprietary information being transferred, uploaded or stored on a home computer, a personal storage device or in a public Cloud outside the protection of the Firm's network, without the approval or authorization of the Firm.

How a personally owned mobile device is used and controlled can impact the privacy and security of the entire Firm and its network and can potentially compromise the Firm's equipment, email and information systems. Malicious applications may be downloaded on a mobile device by its owner, which unintentionally infects the device. Malware can be launched by clicking on links in email attachments or in advertisements on websites which are accessed using the device, which will then attack the device and may seek to access the Firm's network and systems.

Additionally, from time to time it may become necessary for the Firm to preserve and produce electronically stored information (ESI) or emails in the possession of, or under the custody or control of the Firm or its attorneys, irrespective of where that ESI may be stored. As a result, the Firm may need to periodically gain access to a personally owned mobile device, a home computer, a personal storage device, or the Cloud should client or firm information be stored in one of those locations by one the Firm's lawyers. The Firm seeks to avoid, limit, or minimize the need to search home computers, personal storage devices or a non-approved Cloud, and it is in the interests of the Firm and its lawyers to limit or prevent the storage of any Firm or client information on a mobile device, home computer, personal storage device or in any non-approved Cloud.
To comply with various state and federal laws that address the protection of PHI, PII, nonpublic financial information as well as the rules governing the legal profession, which address the protection of client information, attorneys must take reasonable measures to safeguard any information that is either stored, accessed, or transmitted via mobile devices. This data security policy is adopted to protect the Firm's computer network, its information and email systems, and is intended to assist both the Firm and its lawyers in meeting our statutory and ethical obligations to safeguard information. This policy also is intended to prohibit the transfer, upload or storage of Firm or client information to any personally owned mobile device, home computer, personal storage device or non-approved Cloud via a mobile device or otherwise.

Therefore, it is the policy of the Firm that in order for any personally owned mobile device to be linked or granted access to the Firm’s network, email or information systems:

1. The mobile device must be secured by [either (an eight (8) digit PIN,) (biometrics,) or] a strong password with a minimum of [(eight (8))/(twelve (12))] characters, and must include a combination of capitalized or lower case letters, numbers and symbols at the welcome screen level.

2. The password for your mobile device must [comply with the Firm's password policy,] not be a dictionary word or a word easily guessed by someone who knows you, not include or mimic your name or the Firm's name, be used only for that particular mobile device, and not be used for any other purpose.

3. You agree never to share your password for any mobile device with anyone, to not store any password in plain text on the device or to write down any password and leave it in a place where it can be found.

4. Must be configured so that access to the mobile device is locked out after a maximum of [1/2/3] minutes of inactivity requiring a new login.

5. Must be configured to allow the device to automatically lock [or be remotely wiped] if more than [7/8] unsuccessful logins are attempted to gain access to the device.

6. Must remain in the exclusive possession and control of its owner, and as the owner of the mobile device, you agree not to allow any third person to have unsupervised access to the device, or use it in a way that would permit access to any Firm or client information or any PHI or PII that may be stored on the device.
7. Must be configured so that the device is protected by antivirus/anti-malware protection that will periodically scan the device or any applications on the device for the presence of malware.

8. Must be configured so that all information on the device is encrypted.

9. Must have any built-in security features remain in effect on the device. You agree not to attempt to alter or remove any built-in safety features on your mobile device and understand that any attempt to alter the device's built in security, or to jailbreak or root any mobile device that is linked to the Firm’s network, email or information systems is prohibited.

10. The loss or theft of any mobile device linked to the Firm's network, email or information systems must be immediately reported to the Firm’s [Director of IT and General Counsel] immediately upon learning of the loss or theft of that device.

11. You hereby consent and authorize the Firm to take any necessary steps to address the loss or theft of any mobile device owned by you that is linked to the Firm's network, email or information systems, including the remote wiping (deletion) of any information on a lost or stolen device by [the Firm’s IT department].

12. The download of any Firm or client information onto a personally owned mobile device for any purpose is prohibited.

13. The use of any mobile device to send, transfer, store, upload, or backup any Firm or client information to a home or personal computer, to any type of personal storage device, or to [(the) (a non-approved)] Cloud is prohibited.

14. The use of any personal, web-based email account on any mobile device to send, transfer, transmit, store or upload any Firm or client information is prohibited.

15. You agree to notify the Firm’s [Director of IT or (insert person/title)] before selling, disposing or otherwise transferring ownership, control, or possession of any mobile device that is linked to the Firm’s network, email or information systems, and you authorize the Firm to promptly remove or wipe any Firm or client email or information from the device before [or after] selling, disposing or transferring ownership, control, or possession of the device.

[16. Because using the voice-to-text feature of a mobile device can result in the transmission of the spoken words to a third party for review and analysis, you agree not to use the voice-to-text feature of your device to]
draft or send any email or text messages related to a Firm matter, or a Firm client, or that relates or includes the content of any PHI, PII or nonpublic financial information.

[17. Reviewing or sending email or text messages while operating a motor vehicle is prohibited.]

*It is the policy of the Firm that access to the Firm’s network, email and information systems will be blocked immediately upon the effective date of a person’s resignation or termination from the Firm.*

The obligation to preserve client information survives an attorney’s departure from the Firm, and an attorney must continue to safeguard the information stored on any mobile device after the attorney is no longer employed by or associated with the Firm. You agree that the Firm’s IT department can remove any client, Firm, or work-related, email, or information on a mobile device upon notification of a person’s resignation or departure from the Firm. Any attorney or person who resigns from the Firm or is involuntarily terminated by the Firm must temporarily turn the device into [the Firm’s IT department] and allow the removal of any Firm and client information or emails from the device. If a person who is terminated or resigns from the Firm refuses to temporarily turn his or her mobile device into [the Firm’s IT department] for the removal of Firm or client information and emails from the device, the Firm reserves the right to remotely wipe that information from the device, and you hereby consent to having the device wiped, and understand that wiping the device could potentially result in the loss of any personal information you stored on the device.

The failure to follow the Firm's policies on mobile device security can result in discipline up to and including separation from the Firm. A violation of this policy can also result in the immediate termination of your access to the Firm's network, email or information systems via your mobile device.

All other Firm policies including the acceptable use of technology and those prohibiting harassment and discrimination apply to your use of a mobile device and all partners and employees must adhere to them when using a mobile device covered by this policy.

**Consent:** I understand that as a condition of the Firm allowing me to use a personally owned mobile device to gain access to the Firm’s network, email and information systems, I agree to follow the Firm's data security policy for mobile devices, and I expressly consent and hereby authorize the Firm to take whatever steps may be necessary to address the loss or theft of any mobile device that I own, which is/are linked to the Firm's network, email and information systems, including the remote wiping (deletion) of information contained on my device(s) by [our Firm’s IT department]. I further consent and hereby authorize the Firm to remotely wipe the device in the event I resign or am terminated from the Firm and refuse to temporarily
turn the device into [the Firm’s IT department] to allow the removal of Firm and client information and emails from the device. I further consent to allowing the Firm to remove or wipe any Firm related emails or information and any client related information from the device before I sell or transfer possession of the device or should I refuse to temporarily turn the device into [the Firm’s IT department] to allow the removal of Firm and client information and emails from the device. I understand that wiping the device could result in the loss of any personal information stored on my device.

I acknowledge and understand that if I do not secure and configure, or allow the Firm to secure and configure any mobile device as outlined in this policy, and if I do not consent to the remote wiping of any such device(s), that my access to the Firm’s network, email and information systems through any such device(s) will be blocked or terminated.

I further consent and hereby authorize the Firm to recover any Firm or client-related emails or documents from any Cloud, home computer or personal storage device to which those emails or documents were uploaded or stored in violation of this policy. I also consent to the periodic inspection of any mobile device connected to the Firm’s network, email or information systems to ensure compliance with this policy.

Dated: ____________

(print name)

(signature)

* Steven M. Puiszis is a Partner with Hinshaw & Culbertson LLP, and serves as the Firm’s Deputy General Counsel. He is a member of Hinshaw’s Lawyers for the Profession Practice Group which represents lawyers and law firms in liability and professional responsibility matters. Steve also serves as the Firm's privacy and security officer. He is a Fellow of the American Bar Foundation and is a Past President of the Illinois Association of Defense Trial Counsel. He formerly served on the Board of Directors of DRI and as its Secretary Treasurer. His publications include DATA PROTECTION AND PRIVACY IN THE UNITED STATES, and MITIGATING LAW FIRM’S CYBER RISK; separate book chapters published in RISK MANAGEMENT IN LAW FIRMS, Globe Law and Business Publishing Ltd., London, England, sponsored by the International Bar Association; THE ROLE OF GENERAL COUNSEL IN LAW FIRM RISK MANAGEMENT, LAW FIRM PRACTICE MANAGEMENT, the DRI Defense Library Series, DRI, Chicago, Illinois. Steve received his J.D. from Loyola University Chicago.