Legal Ethics and Cybersecurity: Managing Client Confidentiality in the Digital Age

Natasha Babazadeh

ABSTRACT

Lawyers today rely on the Internet and new technology to maintain a competitive edge in the legal market. But staying current comes at a price. As more information is being stored and transferred online, lawyers face new risks and obstacles in upholding their professional responsibilities. The ethical duty to maintain client confidentiality, in particular, has become a rocky terrain in light of increasing cyber threats and data breaches. And, in both the United States and abroad, the current rules of professional responsibility provide little to no guidance for reasonable conduct in the event of a breach, and consequently, fail to ensure that lawyers adequately uphold their duties.

Lawyers play a vital role in protecting client data in the digital age. But the current legal structure fails to hold them accountable. Understanding the obstacles that surround client confidentiality online requires close scrutiny of the strengths and weaknesses of the rules of professional responsibility as they currently stand. This Article proposes that jurisdictions embrace the American Bar Association's approach adopted throughout the United States, but also update these rules to (1) require cybersecurity plans, (2) provide a more concrete definition for "reasonable efforts" to safeguard information, and (3) mandate notice requirements for breaches.

INTRODUCTION

The ethical duty to maintain client confidentiality is essential to the attorney-client relationship and a universally recognized, bedrock common law privilege. With the advent of the Internet and innovation in technology, lawyers conduct an increasing amount of their work

online. Lawyers store client information on personal devices that may be susceptible to remote access and oftentimes, without adequate safeguards, such as authentication and encryption. Thus, in maintaining confidentiality in the digital age, attorneys face new threats and challenges as data breaches proliferate. Rules of professional responsibility throughout the United States and abroad do not adequately address these new threats and the obstacles they present. Consequently, attorney cybersecurity practices are underregulated, compromising client information and fueling public distrust of lawyers and the legal profession more generally.

Understanding, embracing, and confronting the data security issues that lawyers and law firms face today requires an appreciation for the rules of professional responsibility, which represent the unique, self-governing design of the legal profession, and the obligations and responsibilities that flow from it. These rules provide an important perspective on the difficulties of maintaining client confidentiality in the digital age. Lawyers also play a critical role in protecting and maintaining client data in the face of these new technological challenges and cybersecurity threats. By understanding these new obstacles, their consequences, and how an attorney's practice is affected, the better they can prepare for, and respond to, unauthorized access of client information by third parties.

This Article examines how cybersecurity threats and technological advancements in the practice of law can pose serious ethics issues specific to attorneys' duty of confidentiality. Part I emphasizes the lack of regulation in regard to preventing and dealing with cybersecurity threats. Part II discusses the American Bar Association's Model (ABA) Rules of Professional Conduct in the United States and evaluates whether they adequately address cybersecurity threats, and if so, whether they are effective in practice. Part III proceeds by examining and evaluating the ethics rules governing confidentiality in jurisdictions abroad, with a focus on member states of the European Union. Following a comparison of the rules governing professional conduct in the United States with jurisdictions abroad, Part V proposes suggestions for reforming the rules to better protect client data in the digital age, and also offers practical tips for lawyers who are looking to ensure that they are taking reasonable steps in protecting their client's confidential information.

I. BACKGROUND: CONFIDENTIALITY AND CYBERSECURITY

A. Practice: Lawyering and Technology

Like most other professions, technology plays a significant role in the practice of law. Lawyers spend their days, hours on end, sending e-mails, using mobile devices and wireless networks, storing information remotely, and sharing files. Because of lawyers' widespread use of new and developing technologies, they are increasingly facing "unprecedented challenges."[1] The ABA Cybersecurity Handbook explains that "[c]reating, using, communicating, and storing information in electronic form greatly increases the potential for unauthorized access, use, disclosure, and alteration, as well as the risk of loss of destruction."[2] Maintaining client confidentiality has increasingly become more difficult, given the growing use of technology. Lawyers must therefore understand how to take precautions to properly protect client information from hackers, and to mitigate any injuries incurred in the case of a breach.[3]

According to a series of surveys and intelligence reports, there has been an increase in cyber threats to law firms over the last five years. Cyber threats most often take the form of a third party attempting to intercept a network or database to retrieve information without authorization. Many law firms also have been slow in implementing proper cybersecurity measures to ensure adequate data protection.[4] This is particularly true of localized and smaller law firms.[5] Proper

---

[1] ABA Cybersecurity Legal Task Force, Section of Sci. & Tech. Law, Resolution 109, at 4 (2014), http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2014_hod_annual_meeting_109.authcheck dam.pdf [hereinafter ABA Resolution 109].

[2] JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 41 (2013).

[3] Drew T. Simshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data*, 38 AM. J. TRIAL ADVOC. 549, 550 (2015).

[4] BOOZ ALLEN HAMILTON, CYBER4SIGHT SPECIAL REPORT: CYBERTHREATS TO LAW FIRMS (Apr. 14, 2016), https://www.boozallen.com/content/dam/boozallen_site/sig/pdf/white-paper/cyber4sight-special-report-cyberthreats-law-firms.pdf.

[5] *Id.*

cybersecurity measures not only provide protection for external attacks, but they also address other causes of a breach of confidentiality, such as (1) mistakes by the lawyer (e.g., message sent to the wrong person), or (2) illicit access by a known third party (e.g., when a husband gains access to his wife's messages with her attorney in a family or domestic dispute). This Article focuses specifically on external attacks, but also acknowledges the significance of internal and client-side threats posed.

To fully understand how the growing ubiquity of technology and the critical need for cybersecurity awareness has affected the legal profession, the following questions must be answered: How often do breaches occur? Are data breaches more likely to occur in certain legal practices over others? Are they more likely to occur in larger firms, as opposed to solo practitioners? When breaches occur, how often do they injure to the detriment of the firm lawyer, or the client? What types of harms have resulted from these breaches? Who are the individuals or entities that engage in hacking? And why would hackers want to access confidential client information in the first place?

Many of these questions have not and cannot be answered in whole. Firms and lawyers often rarely know when and to what extent their databases have been breached, or whether they are at risk of being breached. Law firms collect and store a wide variety of highly-sensitive data, including personally identifiable information (PII), confidential communications, trade secrets, financial data, and so forth. If there has been a data breach, oftentimes, lawyers and law firms are unsure of what has been taken and whether the breach has caused any harm. They may also face difficulty in discerning attribution, since identifying the source of a breach requires costly expertise that goes above and beyond the skills required to maintain a standard cybersecurity plan. Several companies and organizations, however, have conducted surveys and published reports in this field that shed light on a few of the questions posed, *supra*. Although many cyberattacks and data breaches do not necessarily target or compromise client data, it is important to consider the scope of the cybersecurity threats posed to better understand the risks faced in maintaining the duty of confidentiality in the digital age.

For example, on April 6, 2016, QBE Insurance Group,[6] known for insuring more than one in ten law firms in England and Wales, reported that approximately $120 million was stolen from the legal market within the past eighteen months.[7] Money is not generally protected by confidentiality, but the target sought does not negate the comparable risks and obstacles that lawyers and firms face in protecting their clients' data or, in this case, money. QBE estimated at least 1,500 raids were made on client accounts during the same time, but that only 150 of them were successful.[8] Of the money taken, a small portion was never restored.[9] More generally, on February 24, 2016, TruShield, an IT security company, reported that the legal industry was the third most targeted sector for hacking, after retail and finance.[10] Another group, Cisco Systems Inc., found that the legal industry is the seventh most vulnerable industry to malware in its 2015 Annual Security Report.[11]

The American Bar Association also conducted a report on the extent to which law firms have experienced breaches, based on the available data. Their report found that approximately fifteen percent of all law firms—and twenty-five percent of law firms with at least 100 attorneys—have dealt with a breach because of a "hacker, website

---

[6] QBE is "one of the world's top 20 general insurance and reinsurance companies, with operations in all the key insurance markets." *About QBE*, QBE, https://www.group.qbe.com/about-qbe (last visited Aug. 31, 2018).

[7] *See* John Hyde, *Cyber-Criminals Alarm Insurers as Law Firms Lose £85m*, L. SOC'Y GAZETTE (Apr. 6, 2016), https://www.lawgazette.co.uk/practice/cyber-criminals-alarm-insurers-as-law-firms-lose-85m/5054573.article.

[8] *Id.*

[9] *Id.*

[10] TruShield supported its assertion with a collected data set of nearly fifty billion events. *See* NABEEL AHMED, TRUSHIELD, CYBER THREAT INTELLIGENCE REPORT – JANUARY 2016, (Feb. 25, 2016), https://trushieldinc.com/cyber-threat-intelligence-report-january-2016.

[11] CISCO, 2015 ANNUAL SECURITY REPORT 14 (2015), http://www.cisco.com/c/dam/assets/global/DE/unified_channels/partner_with_cisco/newsletter/2015/edition2/download/cisco-annual-security-report-2015-e.pdf; *see also* William Byrnes, *Most Big Law Firms Have Been Breached, as Hackers Seek Corporate Clients Secrets*, INT'L FIN. L. PROF BLOG (Mar. 24, 2015), http://lawprofessors.typepad.com/intfinlaw/2015/03/most-big-law-firms-have-been-breached-as-hackers-seek-corporate-client-secrets.html.

attack, break-in, or lost or stolen computer or smartphone."[12] In 2012, only ten percent of law firms overall experienced a breach, demonstrating that the threat of breaches has increased by at least five percent just in the past few years.[13] Lastly, the ABA surveyed about 90,000 attorneys in private practice and found that about sixty percent had experienced a breach causing significant disruptions or harm to business, and forty-seven percent said that their firms had no response plan in place to address a security breach when it occurs.[14]

These reports and surveys show how technology is increasingly enabling third parties to access information or assets via unauthorized means. This information may include PII, health or medical records, financial data, trade secrets, and confidential communications, as well as assets, such as trust funds. Lawyers must maintain their duty of confidentiality and competence, but how can lawyers do so when breaching security systems and accessing client information are becoming easier to pull off and much more prevalent? To answer this question, all lawyers should now be required to use simple cybersecurity practices, which can prevent and mitigate the risks of data breaches. To illustrate further, Part I-B. will discuss why law firms have increasingly experienced cyberattacks. Part I-C will then examine how the lack of a regulatory scheme for cybersecurity practices in the legal profession contributes to the growing problem of data breaches affecting client data.

B. Understanding Why Lawyers Experience Cyberattacks

Lawyers and law firms experience cyberattacks for several reasons. Cyberattacks primarily occur because (1) law firms serve as repositories for sensitive and valuable client information, (2) lawyers are usually more "vulnerable" than the lawyer's clients, and (3) lawyers and law firms take advantage of and stay updated on technological

---

[12] Melissa Maleske, *1 in 4 Law Firms are Victims of a Data Breach*, LAW360 (Sept. 22, 2015, 7:16 PM), https://www.law360.com/articles/705657/1-in-4-law-firms-are-victims-of-a-data-breach.

[13] *Id.*

[14] *Id.*

developments, which leads to an increased susceptibility to attacks.[15] Each will be discussed in turn.

1. The Value of Client Information

Law firms experience cyberattacks because they house valuable and extensive records of client information. The ABA Cybersecurity Resolution acknowledged that law firms and lawyers individually "collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-discovery."[16] Law firms also store valuable information for numerous clients; therefore, making it easier and more efficient for hackers to target a firm than to target individual clients. Most important, law firms make for attractive targets because "lawyers are usually involved in only their client's most important business matters, meaning hackers may not need to sift through extraneous data to find the more valuable information."[17] On the one hand, by hacking a law firm, third parties have direct access to extensive critical and valuable information for multiple clients. On the other hand, targeting the individual clients themselves require hackers to engage in more tedious work. Hackers would have to sift through and identify valuable information for that specific individual. Also, hackers would have to engage in a separate cyberattack for each targeted individual, which can be timely, costly, and resource-intensive.

2. The Vulnerability of Law Firms to Cyberattacks

With cyberattacks, lawyers and law firms are more vulnerable than their clients.[18] This vulnerability is also exacerbated for the reason just explained: law firms serve as repositories for valuable information.

---

[15] Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19 CHAP. L. REV. 501, 503–04 (2016).

[16] ABA Resolution 109, *supra* note 1, at 4.

[17] JANE LECLAIR & GREGORY KEELEY, CYBERSECURITY IN OUR DIGITAL LIVES 128 (2015); *see* Simshaw, *supra* note 3, at 550.

[18] *See* LECLAIR & KEELEY, *supra* note 17, at 128; Wald, *supra* note 15, at 505.

Hackers are attracted to law firms because they get more bang for their buck. More important, however, this vulnerability arises from the perception that lawyers "have fewer security resources than their clients,"[19] with less understanding of, and appreciation for, cybersecurity risks.[20] When comparing lawyers with their clients, especially in the corporate arena, clients will often engage in greater cybersecurity practices because clients have more to lose. Clients have a greater incentive to protect their sensitive information than the client's lawyers do, especially since the law firm is just another vendor or source of potential exposure.[21]

This is not to say that lawyers and law firms have no incentive to engage in cybersecurity practices, just that they are less inclined to do so because of the lack of regulation and oversight. Both individual and large corporate clients will also likely always be in a position where they have greater resources and expertise to deal with threats than lawyers.[22] Even with lawyers representing small businesses and individuals, lawyers are still likely more vulnerable, again because clients have more to lose, but also because clients often assume that their information will be protected by attorneys.[23] Because the rules of legal ethics do not adequately regulate or require lawyers to engage in simple cybersecurity practices, lawyers and law firms do not have as much at stake than their clients do. Therefore, hackers are more inclined to target law firms because more often than not, law firms are easier and more vulnerable targets than a law firm's clients.

---

[19] Simshaw, *supra* note 3, at 550. This perception is based on big law firms who are dealing with Fortune 500 companies, such as Google and Facebook, who have tremendous resources and cybersecurity capabilities. Furthermore, because clients have more to lose, they are more likely incentivized to use greater cybersecurity practices.

[20] LECLAIR & KEELEY, *supra* note 17; RHODES & POLLEY, *supra* note 2, at 105 ("Law firms are viewed as a 'very target-rich environment' with significantly less cybersecurity protections in place than their clients have.").

[21] Wald, *supra* note 15, at 506.

[22] *Id.*

[23] *Id.*

3. Reliance on Technology and Susceptibility to Attack

Finally, given competition and the development of technology and its incorporation into the legal profession, lawyers have become vulnerable to cyberattacks.[24] To sustain clients and stay afloat in a competitive legal market, lawyers have been making themselves more available and accessible with technology, particularly with mobile devices they can carry around with them at all times.[25] These devices, such as laptops, tablets and smartphones, besides the pressure for lawyers to resort to outsourcing and artificial intelligence, lead to increased cybersecurity risks and attacks.[26] Lawyers and law firms have become increasingly more vulnerable, therefore, because of technological innovation and the pressure to incorporate such innovations to maintain a competitive edge in the legal market.

C. The Problems Presented by Lack of Regulation

The legal profession requires regulation to ensure compliance with standards designed to protect clients and deter unlawful attorney behavior. As discussed *infra*, a lack of regulation results in insufficient incentives for lawyers to implement the necessary cybersecurity measures to protect their clients' confidential information. Part I-C considers the deficiencies in current regulations governing lawyers' conduct in regard to cybersecurity. Two types of the most common regulations—liability rules and market controls—will be discussed in sequence.

---

[24] *Id.*

[25] Michael McNerney & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, 62 AM. U. L. REV. 1243, 1251 (2013).

[26] *See* Milton C. Regan, Jr. & Palmer T. Heenan, *Supply Chains and Porous Boundaries: The Disaggregation of Legal Services,* 78 FORDHAM L. REV. 2137 (2010); Paul G. Lannon & Phillip M. Schreiber, *BYOD Policies: What Employers Need to Know*, SOC'Y FOR HUMAN RES. MGMT. (Feb. 1, 2016), http://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx.

1. Liability Rules

Clients often rely on liability rules to penalize lawyers who inadequately represent them and to receive a remedy for any incurred damages because of such representation. This is more commonly known as suing for malpractice. In a malpractice suit, a client must satisfy four necessary elements: (1) the existence of a lawyer-client relationship creating a duty by the lawyer, (2) breach of such duty owed, (3) injury proximately caused by the breach; and (4) resulting damages.[27] In regard to regulating lawyer cybersecurity conduct, a client would have a difficult time showing damages. To do so, the client would have to answer the following questions: "who perpetrated the cyberattacks; what information did they steal; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputation damage, resulted for the victim?"[28]

Answering these questions would be nearly impossible or require significant resources and technical expertise. As evidenced by practice, there are hardly any malpractice suits brought for failing to maintain confidentiality because of inadequate cybersecurity practices.[29] Currently, lawyers are under no obligation to report attacks to their clients.[30] Lawyers also are not usually aware that cyberattacks have occurred themselves.[31] Because of the lack of information available to clients regarding breaches, clients cannot bring malpractice suits, contributing to the lack of incentives for lawyers to engage in adequate cybersecurity practices.

2. Market Controls

The typical market controls used for regulating lawyer conduct are also inadequate in the cyber context. Clients are not as likely to

---

[27] Harry F. Mooney & Laurie Styka Bloom, *Anatomy of a Legal Malpractice Claim*, 55 DEF. COUNS. J. 400 (1988).

[28] McNerney & Papadopoulos, *supra* note 25, at 1261.

[29] *Id.* at 1260; *see* Wald, *supra* note 15, at 512.

[30] Simshaw, *supra* note 3, 500–51.

[31] *Id.*

sanction or fire their lawyers when there is a lack of information to justify such actions. For instance, with a breach, it is more often the case that clients do not know the following: "who perpetrated the cyberattack; what information did they steal; what is the value of that information is to them or to others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim."[32] Clients lack sufficient information to take actions against lawyers who fail to maintain confidentiality. Clients also would not even know about a breach or the compromise of their information in the first place.[33] As mentioned above, lawyers need not report attacks to their clients and are usually not even in a position to know that such attacks have occurred. The sheer uncertainty and difficulty in ascertaining sufficient information regarding a data breach contributes towards the inability to regulate keeping client confidentiality in the digital age. This is more apparent, however, with smaller firms and solo-practitioners. As mentioned above, larger institutional clients have greater incentive and perhaps, leverage, to ensure their lawyers practice greater cyber security measures since much more is at stake.

Nonetheless, lawyers face little repercussions for poor performance in implementing cybersecurity measures. The standard market controls that regulate lawyer conduct are generally ineffective. Jurisdictions must amend their rules of professional responsibility, so clients have adequate recourse to address insufficient cybersecurity practices in the case that their personal data is compromised. To be clear, the rules do acknowledge the use of technology in the legal profession, but these acknowledgments are inadequate to properly regulate client confidentiality in the digital age.

II. ABA MODEL RULES ON CONFIDENTIALITY AND CYBERSECURITY

The ABA has advanced several amendments to its Model Rules of Professional Conduct to address technological changes and evolving

[32] Wald, *supra* note 15, at 512.

[33] *Id.* at 502.

security concerns that have impacted the practice of law.[34] In 2012, the ABA Commission on Ethics submitted a Resolution and Report on Technology and Confidentiality to the ABA House of Delegates to provide further guidance to lawyers regarding the use of technology.[35] The ABA House of Delegates approved amendments to Model Rules 1.6, the confidentiality of information, and 1.1, dealing with competency.[36] The discussion that follows argues that, despite the developments in the Rules substance, they still do not adequately address the issues that arise from the duty of confidentiality and cyberattacks compromising client data. Each amendment and the concerns they raise will be discussed in turn.

A. Model Rule 1.6 on Confidentiality of Information

The Rules require lawyers to protect confidential client information, a longstanding legal protection with common law roots. The Rules explain how confidential information is "a fundamental principle . . . contribut[ing] to the trust that is the hallmark of the client-lawyer relationship."[37] This privilege encourages clients "to seek legal assistance and to communicate fully and frankly with the[ir] lawyer even as to embarrassing or legally damaging subject matter" that "the lawyer needs to represent the client effectively."[38] The ABA Cybersecurity Handbook also elaborates that "[t]his obligation to maintain confidentiality of all information concerning a client's representation, no matter the source, is paramount," and "is no less applicable to electronically stored information than to information contained in paper documents or not reduced to any written or stored

---

[34] MODEL RULES OF PROF'L CONDUCT (AM. BAR ASS'N 2018). The Rules serve as a model for regulating attorney ethics and professional responsibility in most U.S. jurisdictions. However, the Rules are not legally binding, and states may promulgate their own rules as well.

[35] ABA Comm'n on Ethics 20/20, Resolution 105A (2012), https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/ 2012_hod_annual_meeting_105a_filed_may_2012.authcheckdam.pdf [hereinafter ABA Resolution 105A].

[36] *Id.*

[37] MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 2 (AM. BAR ASS'N 2018).

[38] *Id.*

form."[39] The importance of maintaining confidentiality has repeatedly been recognized. But do the Rules adequately regulate lawyer cybersecurity practices? The answer is no.

The ABA House of Delegates (Delegates) amended Rule 1.6 to add a paragraph in the notes and amend two comments to account for growing use of technology in the legal profession.[40] The Delegates acknowledged that Rule 1.6 already recognizes a lawyer's duty to take reasonable measures to protect confidential client information from inadvertent or unauthorized disclosures.[41] But they determined that, given growing and pervasive technology to store and transmit confidential information, this existing duty should be explicitly stated in black letter.[42] The Delegates therefore added an additional paragraph to Rule 1.6(c), stating that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[43] What does it mean, however, to "make reasonable efforts" to protect client information while using technology? To address this question, the Delegates revised the comments to further guide lawyers in complying with the amended obligation.[44]

Comments 18 and 19 elaborate on Model Rule 1.6(c)'s obligations. Comment 18 provides that if a lawyer has taken "reasonable efforts" to ensure third parties cannot access or disclose client information is not accessed, any subsequent unauthorized access or disclosure would not violate Rule 1.6(c).[45] The comment emphasizes the central role of reasonableness in determining whether a lawyer's duty is fulfilled. The comment adds that:

> Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are

[39] RHODES & POLLEY, *supra* note 2, at 62.

[40] *See* ABA Resolution 105A, *supra* note 35.

[41] *Id.*

[42] *Id.*

[43] MODEL RULES OF PROF'L CONDUCT r. 1.6(c).

[44] ABA Resolution 105A, *supra* note 35.

[45] MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 18.

> not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[46]

Comment 19 further elaborates on "reasonableness" as it relates to the transmission of "communication that includes information relating to the representation of a client."[47] Referring to confidential information, Comment 19 provides that:

> the lawyer must take *reasonable precautions* to prevent the information from coming into the hands of unintended recipients. . . . Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.[48]

Comments 18 and 19 take the necessary step of clarifying what constitutes "reasonable efforts" in protecting client information. These efforts are crucial to understand the role of lawyers in implementing cybersecurity measures. The comments lay out several important factors, such as the "sensitivity" of client information and the "cost" of implementing safeguards. The comments also provide some context of what courts might look to in determining the "reasonableness" of a lawyer's conduct. The comments do not, however, specify what measures should be adopted or how to best safeguard sensitive client information.

The comments also do not require that lawyers have a cybersecurity plan informing them of appropriate cyberattack prevention methods or breach responses.[49] Because the comments fail to explicitly require this, lawyers will continue to inadequately monitor cyberattacks. This inherent deficiency only works to inhibit a lawyer's ability to take "reasonable efforts" in preparation for, and response to, potential cyberattacks. By not explicitly requiring lawyers to engage in

---

[46] *Id.*

[47] *Id.* cmt. 19.

[48] *Id.* (emphasis added).

[49] Wald, *supra* note 15, at 518.

cybersecurity practices, taking "reasonable efforts" is fruitless. Lawyers will remain ignorant of any breach that has occurred, or information compromised. Lawyers ultimately cannot assess the likelihood of disclosure if additional safeguards are not in place. And lawyers cannot even begin to think about the difficulty in implementing any safeguards since they would have no obligation, or real incentive, to do so. Thus, requiring cybersecurity plans would ensure that lawyers and law firms actively monitor and detect malicious cyber activity and prompt "reasonable precautions" in response.

Even by requiring a cybersecurity plan and elaborating on Rule 1.6(c) in the commentary, the requirement for "reasonable efforts" is still unclear.[50] The Delegates may have purposely left the language and requirements vague to better adapt to growing technology and use. But its failure to provide more guidance may ultimately result in the obligation's futility. Comment 19 also provides that a lawyer's duty to maintain confidentiality "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[51] This refers to ABA Formal Opinion 99-413, where the Standing Committee decided that "[a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the [Model Rules] because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[52] While the commentary fails to expand on "reasonable efforts," subsequent convenings have asserted that using unencrypted e-mail is reasonable because it "affords a reasonable expectation of privacy."[53] This is one instance where the Rule establishes whether commonly practiced conduct is "reasonable." The Rules, however, do not guide lawyers on what additional safeguards they should take.

Lastly, the Model Rules provide no notice requirement. Lawyers have no explicit obligation to report breaches to their clients. Clients would therefore be in the best position to determine whether lawyers are taking "reasonable efforts" to protect client information.

---

[50] *Id.*

[51] MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 19.

[52] ABA Comm'n on Ethics & Prof'l Responsibility, Formal Op. 99–413 (1999) (discussing the duty to maintain confidentiality when using unencrypted e-mail).

[53] Wald, *supra* note 15, at 519.

The clients, however, would not know when or how to evaluate such "reasonable efforts" since they receive no notification if client information is compromised. Without notice, clients cannot investigate a lawyer's "reasonable efforts" to implement data security measures. For all the foregoing reasons, while the Rules have tried to consider growing cyber and technology concerns, these steps are far from sufficient to adequately protect client information.

B. Model Rule 1.1 on Competence

The Rules also have longstanding demand for a duty of competence. Model Rule 1.1 reads: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[54] To emphasize a lawyer's duty of competence, given growing technology, the ABA provided additional language in the commentary. Comment 8 to Model Rule 1.1 states that "a lawyer should *keep abreast* of changes in the law and its practice, including the benefits and risks associated with relevant technology."[55] A lawyer has a "dual role" to promote effective cybersecurity measures, for both the lawyer's own law practice and to benefit the lawyer's clients' businesses.[56]

The ABA Cybersecurity Handbook elaborates further on the necessary actions to fulfill competence, providing that "a lawyer's ethical obligation of competence requires that the lawyer become and remain competent about the technology they use so as to be able to protect client confidential information."[57] The duty also requires "continued vigilance and learning as technology advances, in order to comply with a lawyer's duties under ethics rules."[58] Moreover, if "a lawyer is not competent to decide whether use of a particular technology (e.g., cloud storage, public Wi-Fi) allows reasonable

---

[54] MODEL RULES OF PROF'L CONDUCT r. 1.1 (AM. BAR ASS'N 2018) (emphasis added).

[55] *Id.* cmt. 8 (emphasis added).

[56] Simshaw, *supra* note 3, at 556; *see* LECLAIR & KEELEY, *supra* note 17, at 126.

[57] RHODES & POLLEY, *supra* note 2, at 65.

[58] *Id.* at 66.

measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer."[59]

Comment 8 enables disciplinary action against lawyers. By ignoring developments in technology, lawyers can be deemed incompetent, leading to misconduct and liability. Also, by requiring lawyers to stay current and knowledgeable about technology, lawyers must stay aware of the cyber risks of using such technology and the benefits of implementing security measures. While better than nothing, the comment is still under-inclusive. Comment 8 does not determine whether failing to use technology or nonfeasance in mitigating security risks violates a lawyer's duty of competence.[60] The comment focuses solely on the risks and benefits of "relevant technology."[61] But what does it mean for technology to be relevant? Also, how can one determine if technology is relevant for the duty of competence to apply? Failing to take these questions into consideration contributes to the lack of guidance for lawyers to engage in meaningful cybersecurity practices.

III. RULES OF CONFIDENTIALITY AND CYBERSECURITY IN OTHER JURISDICTIONS

In Europe, each country has its own set of professional responsibility rules that govern legal conduct. The Charter of Core Principles of the European Legal Profession and Code of Conduct for European Lawyers of the Council of Bars and Law Societies in Europe (CCBE) also provides rules for cross-border transactions. In examining individual states within Europe, it is evident that other countries provide little guidance on maintaining client confidentiality in the face of cyber threats or growing technology. But the CCBE provides all states within the European Union a guide on better securing client information in the digital age. This section will discuss the various rules and regulations recognized within individual States and across borders in the European Union, dealing with confidentiality and technology.

---

[59] *Id*.

[60] Wald, *supra* note 15, at 517.

[61] *Id*.

A. European States

1. Germany

In Germany, the Assembly of freely elected representatives adopted a set of Rules of Professional Practice for lawyers.[62] These rules recognized that a lawyer in Germany has the duty and right to maintain client confidentiality.[63] The duty also applies "to all information that becomes known to the [lawyer] . . . in the course of his professional activity and after the [lawyer] . . . has ceased to act for a client."[64] Other than recognizing this duty and defining its scope, the German Rules do not provide guidance of what the duty requires of lawyers, let alone anything related to the duty and its application to developing technology. They also do not mention the word "technology" in any of its provisions. The German Rules thus not only fail to acknowledge a lawyer's use of technology, but also the significant risks technology can impose on maintaining client confidentiality. Consequently, lawyers in Germany likely neither know how to respond to the increasing number of cyberattacks nor what a lawyer's legal duty to secure client information entails.

2. Italy

In Italy, the National Bar Council developed the Code of Conduct for Italian Lawyers to outline the fundamental principles of professional responsibility for its lawyers.[65] Article 28 of the Code, titled "Confidentiality and Professional Secret," sets out the foundation for a lawyer's duty to maintain client confidentiality.[66] Article 28

---

[62] RULES OF PROF'L PRACTICE, (FED. REPUBLIC OF GER. 2018), http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/National_Regulations/DEON_National_CoC/EN_Germany_BORA_Rules_of_Professional_Practice.pdf.

[63] *Id*. at 3.

[64] *Id*.

[65] CODE OF CONDUCT FOR ITALIAN LAWYERS (IT. NAT'L BAR COUNCIL 2014), http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/National_Regulations/DEON_National_CoC/EN_Italy_Code_of_Conduct_for_Italian_Lawyers.pdf.

[66] *Id*.

provides that a lawyer must maintain confidentiality "with regard to the services carried out and to the information which has been given to him by his client or the assisted party, as well as to those he has become aware in circumstances relating to his representation."[67] If a lawyer violates this duty, the lawyer can be subject to "disciplinary sanction and, in such cases where the violation is related to the professional secret, the suspension of the professional practice from one to three years." The Italian Code recognizes the importance of maintaining confidentiality and even provide a section addressing the penalties for failing to uphold the duty. Other than providing a general and ambiguous statement of the duty, however, the Italian Code, like the German Rules, fail to consider cyber threats and implementing security safeguards. It is therefore unclear whether Italian lawyers must engage in effective cybersecurity practices to protect client information under this duty. As a result, lawyer's lack notice of what actions to take to secure client information. And with a lack of notice, the penalty provisions are ineffective.

3. Spain

In Spain, the General Council of the Spanish Bar emphasized the role of confidentiality in its preliminary section of the Code of Conduct, stating "the professional secrecy and confidentiality are duties and rights of the lawyer that are nothing but a specification of the fundamental rights the legal system recognizes for his clients a defense as an essential mechanism of the rule of law."[68] Similar to most other codes of conduct for lawyers around the world, confidentiality in Spain also covers "[a]ll that the client discloses to the lawyer together with all the circumstances, and everything disclosed in a confidential way by the other lawyer."[69] Article 4 of the Code lays out the rules regulating confidence and integrity. Similar to both Germany and Italy,

---

[67] *Id.*

[68] CODE OF CONDUCT OF THE SPANISH BAR (GEN. COUNCIL OF THE SPANISH BAR 2002), http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/National_Regulations/DEON_National_CoC/EN_Spain_Code_of_conduct_of_the_Spanish_Bar.pdf.

[69] *Id.*

Spain only provides a general and ambiguous statement of the duty of confidentiality. It provides that the lawyer is obligated to "not defraud the confidence of his [or] her client and not to defend the interests, which might be in conflict with those of the client."[70] The Spanish Bar also recognizes that a lawyer can waive their other duties in the case, if they might conflict with maintaining confidentiality, particularly in a collective or collaborative setting.[71] The Spanish Code also fails to mention technology or cybersecurity. Therefore, similar to Germany and Italy, Spain does not give proper guidance to lawyers for maintaining confidentiality in the digital age.

B. CCBE Guidance on Improving Cybersecurity

The Council of Bars and Law Societies of Europe (CCBE) Guidance on Improving the IT Security of Lawyers Against Unlawful Surveillance (Guidance) provides CCBE member bars (most European states) advice on keeping client confidentiality from unauthorized access by third parties. Notably, the Guidance is only aspirational, not binding, and contains no enforcement provisions. The CCBE provides "practical guidance to European Bars and Law Societies as to measures which might be taken by individual lawyers and law firms to ensure the adequate protection of material falling under legal professional privilege, professional secrecy and relevant data protection obligations."[72] It addresses the measures lawyers should take to protect themselves and their client information from unauthorized access, and provides the steps a lawyer should take in addressing security issues.[73]

Regarding measures a lawyer should take, the Guidance provides minimum steps for an effective security management

---

[70] *Id*. at 10.

[71] *Id.*

[72] COUNCIL OF BARS & LAW SOCIETIES OF EUR., GUIDANCE ON IMPROVING THE IT SECURITY OF LAWYERS AGAINST UNLAWFUL SURVEILLANCE (2016), http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/IT_LAW/ITL_Guides_recommentations/EN_ITL_20160520_CCBE_Guidance_on_Improving_the_IT_ Security_of_Lawyers_Against_Unlawful_Surveillance.pdf [hereinafter CCBE Guidance].

[73] *Id*.

system.[74] To determine these minimum steps, several factors are considered, including a firm's practice area, its clients, and the skills of its staff. With these factors in mind, a law firm or lawyers should identify its key information assets and services critical to its operation.[75] Therefore, at a minimum, the firm or lawyer should (1) control access to key information assets, (2) define physical security areas with control, (3) secure disposal and removal of equipment, (4) maintain network security, (5) develop operational procedures to ensure protection from malicious code, and (6) manage passwords, back-up and reporting of breaches or other security issues.[76] The Guidance further specifies the use of IT security controls for mobile devices, protection against malware, disposal of media, and more.[77]

The Guidance also addresses security issues, giving an overview of risk-increasing lawyer conduct. To mitigate these risks, the Guidance offers several countermeasures. For example, when communicating with one's client, information is being transmitted through different networks with different capabilities and dangers.[78] While service providers must maintain a level of protection, these providers can also hand over communications to the government or third parties if compelled to do so. Hackers, or individuals with unauthorized access, can also intercept these communications. In order to mitigate the risk posed by third-party interference, the Guidance suggests: (1) encrypting communications, and (2) using non-registered telephones for communications.[79] Using encryption is pretty straightforward and will be discussed further *infra*. Using non-registered telephones is a well-known tactic widely used by perpetrators of terrorist attacks in France—rather than using encryption, just use throwaway phones for communication.[80] While this is a plausible option to mitigate security risks, its controversial use will likely be regulated in the future.

---

[74] *Id*. at 12.
[75] *Id.*
[76] *Id*.
[77] *Id*.
[78] *Id*. at 18.
[79] *Id*. at 18–19.
[80] *Id*. at 19.

The Guidance also highlights access to and use of metadata as a security issue.[81] While the government needs a warrant to retrieve content of communications, no external approval is needed to obtain metadata.[82] Lawyers and law firms also rarely realize when metadata is transferred, and that data, when analyzed, can be very telling. The Guidance recommends lawyers to not use service providers for communicative purposes and use "over-the-top" (OTT) services instead.[83] Using OTT services will ensure no third party recording and storing of information that can later be accessible by third parties.

Lastly, the Guidance emphasizes that absolute protection of client information from unauthorized access of third parties is not feasibly possible.[84] There will always be some unknown vulnerability that might later be exploited. But lawyers still have a duty to remain competent and maintain client confidentiality in the face of these security risks. Lawyers should thus be required to take adequate precautions and measures to mitigate these risks. The Guidance also emphasizes that these duties are constantly evolving since technology and IT systems continue to evolve and new risks and vulnerabilities develop. Individual states within the European Union, like Germany, Italy, and Spain, fail to recognize the use of technology and cyber threats in their codes of legal conduct. The Guidance, however, serves as an aspirational document that European lawyers can rely on to develop greater cybersecurity practices.

---

[81] *Id*.

[82] This is known as the "Third-Party Doctrine," which holds that individuals who voluntarily convey personal information to third-parties (e.g., banks, phone companies, internet service providers, or e-mail servers) no longer have a "reasonable expectation of privacy" in that information. *United States v. Miller*, 425 U.S. 435, 443 (1976) (holding the Fourth Amendment does not protect "information revealed to a third party and conveyed by [that party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

[83] CCBE Guidance*, supra* note 72, at 19. OTT content refers to audio, video, and other forms of media transmitted via the Internet as a standalone product, without an operator of multiple cable or direct-broadcast satellite television systems. *See* Barry Levine, *What Is OTT Programming and Why Does It Matter?*, MARTECH TODAY (July 12, 2016, 12:28 PM), https://martechtoday.com/marketing-landscape-ott-programming-matter-184073.

[84] CCBE Guidance*, supra* note 72, at 24.

IV. CONFIDENTIALITY AND CYBERSECURITY IN THE UNITED STATES AND ABROAD: A COMPARISON

Comparing the United States with the individual European States, it is evident that the United States is further along in implementing professional responsibility rules that consider developing technologies and cyber threats. On the one hand, the ABA amended Model Rules 1.1 and 1.6, dealing with competence and confidentiality, to account for lawyering and technology. The ABA also provided additional commentary to elaborate on a lawyer's duty in these specific areas. Whereas Germany, Italy, and Spain do not mention technology or cyber threats even once throughout their codes of legal conduct. These countries all do, however, impose the duty to maintain client confidentiality. But what does it actually mean to maintain confidentiality in today's digital age? The ABA takes a first stab at answering this question, while Germany, Italy, and Spain still provide little to no guidance.

The ABA, however, does not sufficiently guide lawyers on what security measures they should incorporate into their practice. While the ABA requires lawyers act "reasonably," it neither provides a clear framework for defining "reasonable efforts" nor lays out specific steps or measures attorneys can take to satisfy reasonableness. The CCBE Guidance, however, serves as an exemplar of what should be required of all lawyers around the world. The Guidance suggests steps a lawyer or law firm should take to mitigate security risks. The Guidance also addresses mitigating harm to clients in the case of a breach. But unlike the ABA Model Rules, however, the Guidance is only aspirational and not legally binding on any lawyer or member state. It thus provides neither an enforcement mechanism nor a legal framework to ensure lawyers adequately protect client information.[85]

In an ideal world, the ABA Model Rules would incorporate the CCBE Guidance measures, providing the baseline requirements for lawyer conduct in the digital age. While the ABA mandates that a

[85] *Id*.

lawyer's duty is to keep "abreast of technology," the Guidance provides a lawyer with concrete and practical measures to implement. For instance, the amendment to Rule 1.6 in the ABA states that a lawyer shall "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of" information.[86] The subsequent commentary elaborates that factors for determining reasonableness include: (1) the sensitivity of information, (2) the likelihood of disclosure if additional safeguards aren't used, (3) the cost of employing additional safeguards, (4) the difficulty of implementing safeguards, and (5) the extent to which the safeguards hurt the lawyer's ability to represent the client.[87] The commentary assumes lawyers know which safeguards to use and when. But this assumption is ill-conceived. Without proper guidance and enforcement mechanisms, lawyers will likely continue to fail to implement sufficient cybersecurity practices to safeguard client information.

The CCBE Guidance, however, can help to fill this gap. For example, lawyers frequently must dispose of devices like telephones, laptops, or computers that contain client data.[88] Lawyers must dispose of these devices properly; otherwise, third parties with access to them can restore parts of the data stored on them, compromising confidentiality.[89] The Guidance recognizes this risk and informs lawyers why failing to dispose of devices properly poses as a cyber risk. The Guidance also lays out countermeasures that mitigate the risk, such as ensuring that all data is overwritten or that the devices are physically and completely destroyed.[90] By combining the black letter and commentary of the ABA Model Rules with the Guidance's proposal for concrete action, lawyers will have more clarity of what is expected of them to secure client information. Lawyers will have the capacity and knowledge to uphold the duty of confidentiality in the digital age and can be held accountable should they fall short.

---

[86] MODEL RULES OF PROF'L CONDUCT r. 1.6(c) (AM. BAR ASS'N 2018).

[87] *Id.* r. 1.6 cmt. 19.

[88] CCBE Guidance*, supra* note 72, at 20.

[89] *Id*.

[90] *Id*.

V. SOLUTIONS: REFORM FOR GREATER ACCOUNTABILITY

A. Reforming the Rules

The rules of professional responsibility in the United States and abroad must be reformed to consider cybersecurity and the role that technology plays in the legal profession. Protecting confidential information is a fundamental principle recognized by most, if not all, jurisdictions around the world. This principled duty, however, requires additional safeguards today as it faces new threats. Once, a lawyer's duty to maintain client confidentiality required avoiding negligent disclosure, such as never leaving laptops or notes unattended in public spaces. Such measures are inadequate to uphold that same duty today. Lawyers must take a more proactive role in protecting information against unauthorized access by third parties and other cyber threats.[91] To do so, this Article suggests that jurisdictions take ABA approach in the United States and implement the following reforms: (1) requiring cybersecurity plans, (2) providing a more concrete definition for "reasonable efforts," and (3) mandating notice requirements for breaches.[92] Each will be discussed in turn.

1. Cybersecurity Plan Mandate

The Rules should mandate that lawyers and law offices have cybersecurity plans. Already, ABA Resolution 109 "encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected."[93] The ABA Model Rules, however, do not explicitly require such programs. Lawyers, thus, have no specific obligation to maintain a cybersecurity plan in case of a breach or to implement preventive measures for the unauthorized access of third parties.

---

[91] Wald, *supra* note 15, at 27.

[92] *Id*.

[93] ABA Resolution 109, *supra* note 1.

2. Defining "Reasonable Efforts"

In Model Rule 1.6 on confidentiality, the commentary should provide more concrete guidance to lawyers of what "reasonable efforts" entail. For example, an additional comment could provide that all law firms must employ certain cybersecurity measures, at a minimum, to ensure compliance with the Rules. The comment could also suggest several options so lawyers know what measures are available, such as virus scanners and firewalls, using cryptographically strong passwords, using public cloud providers or file sharing services, avoiding the use of public Wi-Fi, and training employees.[94] Eli Wald proposed a new comment to Rule 1.6 which would ensure that lawyers and law firms were engaging in the minimum to implement security measures:

> Reasonable efforts to prevent the inadvertent or unauthorized disclosure of electronically stored information relating to the representation of a client would normally include robust strategies for identifying, prioritizing, and securing valuable information; periodical inspection of the firm's information storage system for signs of cyberattacks and data theft; the use of basic cybersecurity measures, including the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords updated from time to time, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents; and the adoption of cybersecurity training protocols for firm lawyers and staff.[95]

This amendment would put lawyers on notice. Lawyers will have a better understanding for what constitutes "reasonable efforts" and have discretion over which specific cybersecurity methods to use. The comment would also provide the framework to penalize lawyers for any violations and hold them accountable.

---

[94] Alan W. Ezekiel, Note, *Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft*, 26 HARV. J.L. & TECH. 649 (2013).

[95] Wald, *supra* note 15, at 530.

3. Notice Requirements

Whenever a breach has occurred, or some incident has led to, the compromise of client information, lawyers must report the incident to their clients. The Rules currently do not explicitly require lawyers to give notice, but it does make some references. For example, Comment 18 to Rule 1.6 states that:

> Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or *that impose notification requirements upon the loss of, or unauthorized access to, electronic information*, is beyond the scope of these Rules.[96]

This comment makes it seem as though notice requirements are beyond the scope of the Rules; however, the comment should be read narrowly to provide that "other law" has the possibility of imposing additional duties outside of the Rules.[97] Having a notice provision in the Rules would complement the other proposals and ensure that market controls can become a more effective way to regulate lawyers. By receiving notice, clients can respond to cyber breaches to better protect their information or mitigate the harm. Clients can also serve as a check on lawyers or law firms to ensure "reasonable efforts" have been taken to protect their information.

B. Practical Tips

Lawyers and law firms can utilize some practical tips to mitigate the risks of unauthorized access to client information. These tips include the use of password protection, encryption, and mobile security. Each will be discussed in turn.

---

[96] MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. (AM. BAR ASS'N 2018) (emphasis added).

[97] Wald, *supra* note 15, at 536.

1. Password Fundamentals for Protection

The simplest measure that any lawyer can take to better secure client information is to use password protection and to use it smartly. A password can require work, such as remembering the password and spending time to type it in. But it is worth it. A password can reduce risks of unauthorized access to client information.[98] The stronger the password, the better—the less likely a third party can guess it or break its code. What constitutes a strong password? Strong passwords normally do not involve commonly used passwords, such as "password" or "123456."[99] Any password that someone could guess is not a strong password. Strong passwords should contain a combination of uppercase and lowercase letters, numbers, and symbols, and should be at least eight characters long.[100]

In the past, one tip for better remembering passwords was to replace letters with symbols or numbers—for example, P@55w0rD.[101] This may not be as effective given how standard the practice has become and how affordable it is to build password cracking tools that can try tens of millions of possible passwords.[102] Experts now, however, have recommended a collection of words or phrases that is easy to remember, for example, the opening line to your favorite joke.[103] Longer passwords are better because each additional figure makes it increasingly more difficult to attack via brute-force methods.[104] Also, the same passwords should not be used more than once or twice. If a hacker discovered your password for one device, the hacker would then have access to any of the others if there are no

[98] J.S. Christie Jr., *Ethics in the Tech Age: What Every Lawyer Should Consider*, LAW360 (April 1, 2015, 12:00 AM), https://www.law360.com/articles/637991/ethics-in-the-tech-age-what-every-lawyer-should-consider.

[99] Morgan, *Announcing Our Worst Passwords of 2016*, TEAMSID (Jan. 22, 2017), https://www.teamsid.com/worst-passwords-2016/?nabe=4587092537769984:3,6610887771422720:0&utm_referrer=https%3A%2F%2Fwww.google.com%2F.

[100] Christie Jr., *supra* note 98.

[101] *Id*.

[102] *Password Do's and Don'ts*, KREBS SECURITY, https://krebsonsecurity.com/password-dos-and-donts (last visited Sept. 12, 2018).

[103] *Id.*

[104] *Id.*

changes made among devices and services. There are also applications, like LastPass, that provide password managers to help create strong passwords and remember them.[105] A lawyer must be mindful that using third party password managers and online applications also creates another venue for hackers to break through. But the cost is worth the benefit since a password manager also significantly reduces other attack surfaces. To mitigate any additional risks, lawyers should keep passwords in a remote location, inaccessible by a network third parties could intercept or a physical location someone could pass upon.

2. Computer System Security and Encryption

For greater security in transmitting information to and from your client and other third parties, lawyers must practice using encryption. Depending on the type of information, lawyers can use encryption as an additional security feature for more sensitive data. There are currently a lot of encryption tools that are built in to e-mail services, including the Microsoft Office Suite and even the G-Suite, but lawyers must also engage in their own separate analysis and practice of encrypting client communications and data when appropriate. Encryption requires encoding data, so hackers cannot read it, but parties who are provided the key can decode it.[106] Even the most technologically savvy hackers have a difficult time deciphering encrypted data without having the key.[107] In an instance where a hacker does obtain access to the key, lawyers and clients should also utilize authentication safeguards. Authentication verifies the identity of the person with access to the key, denying any unauthorized third parties from using the key.[108] Therefore, by encrypting data and implementing

---

[105] *#1 Password Manager, Vault, & Digital Wallet App*, LASTPASS, https://www.lastpass.com (last visited Nov. 28, 2018).

[106] *FYI: Playing it Safe With Encryption*, ABA: TECH OVERVIEW & CHARTS (July 6, 2015), https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/FYI_Playing_it_safe.html; *see* Christie Jr., *supra* note 100.

[107] *Id*.

[108] *See Understanding Authentication, Authorization, and Encryption,* BU TECHWEB, https://www.bu.edu/tech/about/security-resources/bestpractice/auth (last visited Sept. 12, 2018).

authentication safeguards, unauthorized third parties who intercept the data cannot use it.

However, encrypting all communications all the time is not an efficient use of one's time or resources. Lawyers must distinguish between very sensitive information and information that is not likely a target for third party hackers. There are also some email programs that automatically encrypt data when sent, so that one need not go through the extra effort to encrypt and decrypt the data themselves.[109] Therefore, by practicing encryption, lawyers will significantly reduce the risk of compromising client information.

3. Mobile Device Security

Mobile device security refers to the risks lawyers face by losing portable devices, such as laptops, tablets, smartphones, or the interception of these devices through Wi-Fi.[110] Both password protection and encryption, mentioned above, can help to better secure these devices from physical or electronic intrusion. But some other useful practices to ensure mobile security include: remote wiping, two-factor identification, inactivity timeouts, and automatic wiping if access has been denied a specific number of times.[111] Multi-factor identification, in particular, warrants some additional attention. Multi-factor identification is a common service offered by vendors that lawyers are likely to be exposed to, such as Microsoft, G-Suite, financial institutions and so forth. As mentioned earlier, authentication serves as an added layer of protection against unauthorized third parties. There is a big push in the security community, however, away from SMS-based two factor, which has been rendered insecure,[112] and

---

[109] *See id.* For example, Microsoft Exchange provides encryption services for all emails that are being transmitted from this forum. *Id*.

[110] *Id.*

[111] *Id*.

[112] *See* Russell Brandom, *This Is Why You Shouldn't Use Texts for Two-Factor Authentication*, VERGE (Sept. 18, 2017, 1:17 PM), https://www.theverge.com/2017/9/18/16328172/sms-two-factor-authentication-hack-password-bitcoin; *see also* Lily Hay Newman, *Reddit Got Hacked Thanks to a Woefully Insecure Two-Factor Setup*, WIRED (Aug. 1, 2018, 4:38 PM), https://www.wired.com/story/reddit-hacked-thanks-to-woefully-insecure-two-factor-setup.

towards dedicated authentication apps (e.g., Google Authenticator, RSA, Duo, etc.) and services.[113]

Lawyers should be aware of mobile security when they use Wi-Fi services, especially in a coffee shop or hotel. When using Wi-Fi, third parties can intercept data being sent between the device and the hotspot that provides the service.[114] So, if a lawyer works remotely and uses a local Wi-Fi network to access the Internet, then the lawyer is potentially jeopardizing their clients' confidentiality. Lawyers can mitigate this risk by using encryption, or several of the other features previously discussed.

Otherwise, the best decision for a lawyer is to avoid Wi-Fi networks in public spaces completely. An alternative to Wi-Fi is using a virtual private network (VPN) connection to a firm's network. A law firm providing Wi-Fi access to its guests, however, should limit their access to a different network than the one the law firm relies on.[115] Also, the guest network should only be provided to clients if they are appropriately protected and trustworthy.[116] Regarding information storage, using cloud services can be more secure than relying on a lawyer's own network and systems. For example, a commonly used cloud service system is Dropbox. Dropbox uses encryption and two-step verification to prevent unauthorized access to the information contained within. Taking these practical tips into consideration, a lawyer can more adequately maintain client confidentiality in the digital age.

VI. CONCLUSION

Given the lack of regulation, market pressures, and uncertainty in detection, attribution, and probing the scope of harm caused by cyberattacks, the professional rules of responsibility in the legal profession are often inadequate to regulate lawyer conduct. These rules,

---

[113] *See About: What is FIDO?*, FIDO ALL., https://fidoalliance.org/about/what-is-fido (last visited Sept. 12, 2018). The FIDO Alliance provides specification and certifications for an interoperable ecosystem that supports a wide range of authenticator technologies. *Id.*

[114] *Id.*

[115] CCBE Guidance, *supra* note 72, at 21.

[116] *Id*.

in the United States and abroad, still can play a meaningful role in incentivizing lawyers to adopt risk mitigation measures and implement preventative cybersecurity plans. Also, lawyers must demonstrate to their clients and the public at large themselves that they are taking measures to provide greater security for their practice. For this reason, any rules regulating their use of technology should also incorporate guidelines defining risky behavior and reasonable conduct.

Lawyers and law firms should stay educated, foster a cyber conscious culture, and seek outside aid when necessary. They must also utilize practical security measures, such as strong and unique passwords, encryption, and multi-factor identification. Embracing a more conscientious and proactive cybersecurity practice ensures a future in which lawyers can continue to adequately maintain client confidentiality, while ensuring clients can continue to depend on the legal profession for competent services.