Arizona Law Journal of Emerging Technologies

Volume 7 *Article 4*

5-2024

ADJUSTING THE LEGAL PROFESSION'S PRIVACY RESPONSIBILITIES TO KEEP UP WITH TECHNOLOGICAL CHANGES

Kristin Wolek
University of Arizona James E. Rogers College of Law

2023-2024 https://azlawjet.com Vol. 7, Art. 4

Arizona Law Journal of Emerging Technologies

ADJUSTING THE LEGAL PROFESSION'S PRIVACY RESPONSIBILITIES TO KEEP UP WITH TECHNOLOGICAL CHANGES

Kristin Wolek, J.D.

Table of Contents

ADJUSTING THE LEGAL PROFESSION'S PRIVACY RESPONSIBILITIES TO KEEP UP WITH TECHNOLOGICAL CHANGES

Kristin Wolek*

I. Background

In 2020, a group of hackers known as REvil took control of a law firm's data for ransom.[1] This law firm was Grubman Shire Meiselas and Sacks, an entertainment law firm with many high-profile clients and a reputation to protect.[2] REvil threatened to release a huge quantity of information related to the representation of the firm's celebrity clients unless they were paid $42 million in ransom.[3] Ultimately, Revil released several gigabytes of confidential legal information onto the dark web.[4] Much of this information is still being circulated online, affecting the privacy of the firm's clients and the well-being of the firm itself.[5] According to an expert in cyber security, "…there is no guarantee if they pay the ransom in full the documents won't get leaked anyway. The reputational damage is already done. I'm also sure the firm is keenly aware of the potential legal issues they are facing."[6]

The attack on Grubman Shire Meiselas and Sacks could have been prevented. The hackers used a malware called Sodinokibi to initiate their attack.[7] Over a year before this attack occurred, Sodinokibi had already been used to attack other businesses, and information about this malware was publicly accessible.[8] Other firms could have looked into these attacks and figured out what sort of security vulnerability Sodinokibi was known to take advantage of. The malware still went undetected, likely entering the firm's systems via email or unsecured networks.[9] This attack caused severe damage to the clients, the clients' associates, and the law firm itself.[10] A privacy breach this severe must be avoided at all costs, yet Grubman Shire Meiselas and Sacks was not as prepared as they could have been. It does not appear they attempted to take any steps to protect themselves against a Sodinokibi attack.[11] REvil took advantage of gaps in their security in order to commit

* J.D., University of Arizona James E. Rogers College of Law, May 2023.
[1] Akshaya Asokan, *Ransomware Gang Demands $42 Million From Celebrity Law Firm*, DATA BREACH TODAY (May 16, 2020), https://www.databreachtoday.com/ransomware-gang-demands-42-million-from-celebrity-law-firm-a-14292.
[2] *Id.*
[3] *Id.*
[4] *Id.*
[5] *See id.*
[6] *Id.*
[7] Byron Mühlberg, *Ransomware Attack Hits One Public Figure After Another*, CPO MAGAZINE (May 26, 2020), https://www.cpomagazine.com/cyber-security/ransomware-attack-hits-one-public-figure-after-another/.
[8] Greg Belding, *Malware Spotlight: Sodinokibi*, INFOSEC (Apr. 9 2020), https://resources.infosecinstitute.com/topic/malware-spotlight-sodinokibi/.
[9] *See id.*
[10] Asokan, *supra* note 1.
[11] *Id.*

their cyber-attack.[12] This is not the only attack caused by vulnerabilities in the technology used by a law firm, and it will not be the last.[13] Legal professionals must consider not only how they might prevent a breach in their practice, but also how the legal profession as a whole must work to protect privacy.

Privacy is extremely important in any industry, but it is especially important to protect in the legal profession. Privacy and all of its complexities are something any person involved in the profession should consider. Privacy is sometimes considered a right, and other times it is considered part of other rights;[14] this can make privacy litigation complicated. People believe a right to privacy arises out of the U.S. Constitution, even when a right to privacy is not described directly, causing many Americans to expect and value privacy.[15] Certain Supreme Court cases, such as *Griswold v. Connecticut*, a case striking down a law that interfered with the privacy of married couples, have given a right to privacy.[16] Since then, a general right to privacy has been upheld in multiple cases and is often considered something granted by the Constitution.[17] While this right has become more contested recently,[18] it is still a right that many people expect to have.[19] As a society, we are aware of how much someone can be hurt when their privacy is violated. A lack of privacy, or even a perceived lack of privacy, will impact people. One consequence that often comes with a lack of privacy is a chilling effect, which may make someone reluctant to speak freely or share information in general.[20] Most people have some expectation of privacy, potentially more so in certain situations, such as when someone is giving sensitive information to a legal professional that they hope will help them with their legal problems.[21] Privacy is a right that is important to a lot of people and is especially important in getting people to feel safe in their interactions with certain professionals.

Privacy is something that legal professionals must always consider. There is an important relationship between privacy and professional responsibility, especially in the legal profession.[22] Lawyers and law firms have strong obligations regarding privacy, and privacy is often expected of them by people who seek out legal advice and representation.[23] Privacy and confidentiality are especially important since the legal profession deals with sensitive information that is often crucial to the practice of law; anything that interrupts this flow of information could damage the legal profession. Several rules in the Model Rules of Professional Conduct (MRPC) refer to the right to privacy for different people involved in the practice of law.[24] Legal information is often confidential, and legal professionals are obligated not to share it.[25] Privacy is especially

[12] *See id.*; *see* Mühlberg, *supra* note 7.
[13] Asokan, *supra* note 1.
[14] Judith Wagner DeCew, *The Scope of Privacy in Law and Ethics*, 5 Law and Phil. 145, 149 (1986).
[15] *See id.* at 146-147, 169-170, 173.
[16] 381 U.S. 479, 486 (1965).
[17] *DeCew*, *supra* note 14, at 159.
[18] *See generally* Dobbs v. Jackson Women's Health Org., 597 U.S. 215, 217 (2022).
[19] Colleen McClain et al., *How Americans View Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/.
[20] Trina J. Magi, *Fourteen Reasons Privacy Matters: A Multidisciplinary Review of Scholarly Literature*, 81 LIBRARY Q. 187, 188 (2011).
[21] Micah Schwartzbach, *The Attorney-Client Privilege*, NOLO, https://www.nolo.com/legal-encyclopedia/attorney-client-privilege.html (last accessed Apr. 20, 2024).
[22] *See* MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 1983).
[23] *Id.*
[24] *See, e.g.*, *Id.* at r. 1.6; *Id.* at r. 1.18; *Id.* at r. 1.9.
[25] *Id.* at r. 1.6.

important for a lawyer's client; when a person gives information to their lawyer, it is considered the lawyer's professional responsibility to keep that information confidential.[26] This does not only include protecting the client's information but also more broadly, all communications between the lawyer and their clients.[27]

Confidentiality is a key part of the lawyer-client relationship.[28] In order for the relationship to function properly, a client needs to be able to speak freely with their lawyer and to trust that this information will not be shared.[29] If a client does not believe their information will be kept private, they may be less inclined to share information, even if it is relevant to their legal goal. Information is powerful in legal proceedings. A lawyer needs all the pertinent information pertaining to their client's legal matter in order to represent them competently.[30] Another potential harm is that if people do not trust lawyers' ability to protect sensitive information, then they may even be less likely to seek legal help altogether.

Ultimately, lawyers have a special obligation to protect their client's information to uphold and maintain their trust. To that end, a lawyer should not intentionally share any sensitive information, but should also take reasonable precautions in order to protect information from getting leaked.[31] Any information leak or breach of privacy is not only harmful overall to the person, but is harmful to the relationship between lawyers and clients.[32] In addition to the obligations that a lawyer has towards their client, a lawyer also has obligations towards third parties. Generally, these obligations focus on not doing anything to bring unnecessary harm upon third parties or to infringe upon their rights, which could include the third party's right to privacy.[33] According to the Model Rules of Professional Conduct, a lawyer must not obtain any information about a third party that would violate their rights.[34] Legal professionals must attempt to uphold privacy, both out of ethical obligations and in order for key aspects of the legal profession to function.

Protecting privacy is rarely simple. Privacy is a right that has significant limitations, especially where legal actions are concerned. For example, there are situations in which privacy laws may be relaxed, especially when it comes to criminal activity.[35] In these instances, information being shared may not necessarily be considered a breach of ethics.[36] Moreover, there are situations in which a lawyer may be allowed to violate their duty of confidentiality, such as when they have confidential information that would

[26] *See id.*
[27] Timothy J. Toohey, *Beyond Technophobia: Lawyers' Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks*, 21 RICH. J. L. & TECH. 9, 13 (2015).
[28] *See* MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 1983).
[29] Wex Definitions Team, *Attorney's Duty of Confidentiality*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/attorney's_duty_of_confidentiality (last updated June 2022).
[30] *See* MODEL RULES OF PRO. CONDUCT r. 1.1 (AM. BAR ASS'N 1983).
[31] *Id.* at cmt. 8.
[32] Toohey, *supra* note 27, at 1; Andrew Conte, *Unprepared Law Firms Vulnerable to Hackers*, TRIBLIVE (Sept. 13, 2014, 10:40 PM), https://archive.triblive.com/local/pittsburgh-allegheny/unprepared-law-firms-vulnerable-to-hackers-2/#axzz3S2IsKaPf [https://perma.cc/9DUR-HQXF].
[33] *E.g.*, Aviva M. Kaiser, *Respecting Others' Privileged Information: Lawyers' Obligations to Third Persons*, STATE BAR OF WIS.: WISCONSINLAWYER (Apr. 1, 2017), https://www.wisbar.org/NewsPublications/WisconsinLawyer/Pages/Article.aspx?ArticleID=25528.
[34] MODEL RULES OF PRO. CONDUCT r. 4.4 (AM. BAR ASS'N 1983).
[35] *See, e.g.*, *661. Privacy Protection Act of 1980*, JUSTICE, https://www.justice.gov/archives/jm/criminal-resource-manual-661-privacy-protection-act-1980 (last accessed April 20, 2024).
[36] *See generally id.*

prevent harm to another person.[37] In these instances, it can be complicated for lawyers to assess the nuances of the situation, especially when their client shares information—in confidence—about criminal activity.[38] Thus, an ethical lawyer must often consider how to properly and ethically use the sensitive and private information they obtain.

The obligations lawyers have regarding information are very serious. A breach of privacy ethics could have a drastic impact on individual clients and on the practice of law in general. The legal profession remains fairly traditional compared to other industries, and as a result, modern technology is something many lawyers may not be especially knowledgeable about.[39] Legal professionals may not understand the risks associated with this technology, especially when it comes to cyber security.[40] However, they must learn about technology and the ways in which it may impact privacy in the legal field in order to uphold legal ethics.[41]

II. Issues and Current Standards

Changing technology has made privacy issues more complex and has created new ethical problems. Protecting privacy now requires more technological awareness than it may have previously. More information is being stored on the Internet, often on an online cloud.[42] Information being stored digitally and online can lead to an increased risk of privacy breaches. This may occur for a number of reasons, including cyber security attacks or user errors.[43] For example, a hacker may find a way to gain access to a law firm's data, or a lawyer may make a careless mistake that leads to data being exposed.[44] This might occur as a result of a lack of sufficient network security, or from a lawyer simply sending an email to the wrong person.[45] As a result of information being stored on the Internet, the information can potentially be accessed from a wider variety of locations.[46] This potentially increases points of access that require protection, and thus, legal professionals shall be acutely aware of the potential security vulnerabilities that may arise.

Cyber security is a growing issue that has not been adequately addressed in the legal field. Many lawyers are uninformed about how to best protect digital information from cyber-attacks.[47] Even if they have heard about cyber security being important in other industries, they may not understand that a law firm is just as vulnerable to a cyber-attack, if not more so, than any other business.[48] With the increase in digital data, a cyber security breach can cause severe privacy issues. If proper cyber security precautions are not taken, it will

[37] *Attorney's Duty of Confidentiality, supra* note 29.
[38] *See* Judith Wagner DeCew, *The Scope of Privacy in Law and Ethics*, 5 L. & PHIL. 145, 1466 (1986).
[39] Toohey, *supra* note 27, at 4.
[40] *Id.* at 6.
[41] *See* MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 1983).
[42] Natasha Babazadeh, *Legal Ethics and Cybersecurity: Managing Client Confidentiality in the Digital Age*, 7 J. L. & CYBER WARFARE 85, 110 (2018); Toohey, *supra* note 27, at 2-3.
[43] Tim Maurer & Garrett Hinck, *Cloud Security: A Primer for Policymakers* 2, 4, 26 (Carnegie Endowment for International Peace, Working Paper, 2020).
[44] Toohey, *supra* note 27, at 24.
[45] *Id.*
[46] *Id.*
[47] Babazadeh, *supra* note 42, at 92.
[48] Toohey, *supra* note 27, at 4-5.

be more possible for a hacker to expose the data of lawyers or law firms.[49] Cyber security in the legal profession is largely unregulated and the guidelines for cyber security are vague- lawyers have to make reasonable efforts to keep up with cyber security practices, but law firms may not train their lawyers about cyber security.[50] This increases the chance for potential breaches.[51] Many law firms, especially smaller law firms, have been slow to adopt good cyber security practices, which makes them vulnerable to hackers and cyber-attacks.[52] Arguably, knowledge of current cyber security issues is required by Section 1.6 of the Model Rules of Professional Responsibility, which discusses confidentiality.[53] The ABA's guidelines state that a lawyer must make reasonable efforts in order to prevent unauthorized access to the client's information, which may include cyber security precautions.[54] However, it is unclear exactly how far "reasonable efforts" would extend and its associated obligations.[55] Many lawyers are not especially knowledgeable about cyber security and are often not expected to be.[56]

Furthermore, there are other privacy concerns that can arise out of new technology, even when what occurs would not typically be considered a cyber security breach. A privacy breach may occur even without a hacker or other malicious actor.[57] Many communications between a lawyer and client will be through email. These technologies make it easy for mistakes to happen, leading to breaches in privacy.[58] A lawyer might prepare an email that contains sensitive information and send it to the wrong person, and thus, unintentionally revealing confidential information.[59] There are also concerns about information that may be unintentionally attached to an email or to a file that is being shared- this is especially likely to occur with the increase in metadata, which causes information to be passively attached to files and emails.[60]

a. Forms of Cyber Security Breaches

Cyber security is a growing concern, as more businesses rely on digital technology and are susceptible to cyber-attacks. Cyber security breaches can occur in a number of ways that law firms may not be prepared for. This includes phishing, where "a target or targets are contacted by email, telephone or text message by someone posing as a legitimate

[49] Babazadeh, *supra* note 42, at 108.
[50] *See generally* Teresa Matich, *2024 Law Firm Data Security Guide: How to Keep Your Law Firm Secure*, CLIO, https://www.clio.com/blog/data-security-law-firms/ (last accessed Apr. 20, 2024).
[51] *See id.*
[52] Daniel B. Garrie et al., *Small Law Firms Must Take Action and Address Cybersecurity and Privacy Regulations,* ALM: LEGALTECH NEWS (Feb. 15, 2024), https://www.law.com/legaltechnews/2024/02/15/small-law-firms-must-take-action-and-address-cybersecurity-and-privacy-regulations.
[53] *See* MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 1983).
[54] *See* John P. Ratnaswamy, *Ethics 20/20 and Confidentiality*, 29 PRIV. & CONFIDENTIALITY 40, 42 (2012).
[55] *See generally* MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 1983).
[56] Toohey, *supra* note 27, at 4-5.
[57] *See Protecting Your Law Firm's Reputation: Tips to Prevent Accidentally Sending Confidential Client Information Via Email*, VIPRE SAFESEND (June 15, 2023), https://safesendsoftware.com/protecting-your-law-firms-reputation/.
[58] *See id.*
[59] Babazadeh, *supra* note 42, at 108; Megan E. McEnroe, *E-Mail in Attorney-Client Communications: A Survey of Significant Developments April 2009—June 2010*, 66 BUS. LAW. 191, 192 (2010).
[60] Dave Kinsey, *Ethics and Metadata: What Law Firms Need to Understand*, ATT'Y L. MAG. (Oct. 23, 2016), https://attorneyatlawmagazine.com/practice-management/legal-ethics/ethics-and-metadata-what-law-firms-need-to-understand.

institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts."[61] Essentially, this is a way cybercriminals could be given sensitive information or even obtain login details in order to gain access to a law firm's data.[62] In 2016, there was a massive phishing attempt committed by a Russian hacker that targeted many top US law firms.[63] It is possible this led to massive security breaches due to the law firms lacking sophisticated cybersecurity systems,[64] or not training their lawyers about cyber security and spotting phishing schemes. Lawyers should be acutely aware of these threats and should be motivated to protect information against them.

Ransomware is a cyber security issue that law firms must be aware of and be prepared to deal with. In 2022, 17% of cyber-attacks involved ransomware.[65] Also, different types of cyber-attacks are connected, as ransomware can sometimes occur from a hacker gaining access to someone's systems via phishing.[66] Typically, ransomware involves the installation of a program, which then makes the network or computers unusable until some amount of money is paid.[67] There is often also a threat that data will be released or otherwise stolen if the ransom is not paid.[68] Someone may be tricked into installing ransomware, potentially via phishing or by the software being attached to a program that appears legitimate.[69] At times, ransomware may be used to access data and threaten to release that data if the owners do not comply, which is what occurred during REvil's attack on Grubman Shire Meiselas and Sacks.[70] In light of the multiple instances of legal data being seized and held for ransom by hackers,[71] law firms suffer financially because breaches involving ransomware are very costly. Even if one excludes the cost of the ransom payment itself, it is estimated that a ransomware attack costs $4.62 million on average.[72]

Big data has created ethical issues. Due to new technology, massive amounts of information is being collected by many industries; much of this information has the

[61] *What Is Phishing?*, PHISHING, https://www.phishing.org/what-is-phishing (last visited Apr. 20, 2024).
[62] *Id.*
[63] Sharon D. Nelson, *Russian Cybercriminal Aims to Breach Top U.S. Law Firms,* SENSEI ENTERS. (Apr. 4, 2016), https://senseient.com/ride-the-lightning/russian-cybercriminal-aims-to-breach-top-us-law-firms/.
[64] *See Russian Cybercriminals Target 50 Law Firms Nationwide*, CIAB, https://www.ciab.com/resources/russian-cybercriminals-target-50-law-firms-nationwide/ (last accessed Apr. 20, 2024).
[65] *What Is Ransomware?*, IBM (2022), https://www.ibm.com/topics/ransomware (last visited Apr. 20, 2024).
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] Akshaya Asokan, *Ransomware Gang Demands $42 Million From Celebrity Law Firm*, DATA BREACH TODAY (May 16, 2020), https://www.databreachtoday.com/ransomware-gang-demands-42-million-from-celebrity-law-firm-a-14292.
[71] *E.g.*, Y. Peter Kang, *'Cryptolocker' Virus Holding Law Firm Data for Ransom*, LAW360 (Mar. 9, 2015, 6:49 PM), http://www.law360.com/articles/629305/cryptolocker-virusholding-law-firm-data-for-ransom; Isha Marathe, *The Dark Side of Tech: 8 Law Firms That Suffered Data Breaches in 2023*, ALM L.: LEGALTECH NEWS (Dec. 21, 2023, 2:59 PM), https://www.law.com/legaltechnews/2023/12/21/the-dark-side-of-tech-8-law-firms-that-suffered-data-breaches-in-2023/.
[72] *The True Cost of a Ransomware Attack*, CYBELANGEL, https://cybelangel.com/the-true-cost-of-a-ransomware-attack/ (last visited Apr. 20, 2024).

potential to be relevant to legal professionals.[73] This has created unprecedented problems, even in industries that have always dealt with data, as data of this quantity cannot be dealt with via traditional data processing software.[74] Oftentimes, there is a large amount of data that is created unintentionally—such as metadata that may be attached to files or emails—and a person may be unaware of the information they are sharing.[75] While much of this data may be useful in practicing law, it also comes with various ethical concerns. This includes data that may be privileged information in other fields; lawyers must consider the ethical obligations of these fields as well.[76] One example of data that is now available to more people is psychological test data, which is often intended to only be used for mental health treatments and would not be expected to be utilized in the legal practice.[77] The excess of data allows for more analytical decisions. However, it also opens up ethical questions regarding how much data should be used, and for what purposes.[78] There is an increased risk of evidence being collected that may contain information that would risk violating the privacy of third parties.[79]

Another important aspect of information that has emerged due to new technology is metadata. Metadata is information attached to data, sometimes without the person being informed that this information is being shared.[80] The concept of metadata and the lack of awareness about it, especially in the legal profession, means that it is easier for information to be transmitted unintentionally.[81] Various information might be included in metadata.[82] This can include the original author of a document, the location that a photo was taken, the edit history of a file, and more.[83] There are generally less regulations surrounding metadata than there are surrounding regular data, and the ABA has not provided many guidelines regarding metadata.[84] This makes a lawyer's obligations regarding metadata even less clear than other forms of information. This is made more difficult when a lawyer does not know about metadata and is unaware of what kind of information they may be giving away by not carefully considering the metadata of any documents, emails, or other files that they may be sharing.

b. Technology and the Practice of Law

Many people in the legal profession are not knowledgeable about technology in general,

[73] *Big Data: What It Is and Why It Matters*, SAS, https://www.sas.com/en_us/insights/big-data/what-is-big-data.html (last visited Apr. 20, 2024).
[74] *Id.*
[75] *See generally* Bennett B. Borden, *Big Data, Analytics and Ethics: Lawyering in the Information Age*, NAT'L COMM. ON VITAL & HEALTH STAT. 1-3 (2017), https://ncvhs.hhs.gov/wp-content/uploads/2017/11/B3-Bennett-Borden-PCS-2017Nov28-Big-Data-Analytics-and-Ethics-Lawyering-in-the-Information-Age-508.pdf.
[76] *See generally* ERIC Y. DROGIN, ETHICAL CONFLICTS IN PSYCHOLOGY 257 (Am. Psych. Ass'n, 5th ed. 2019).
[77] *See id.*
[78] *See generally* Borden, *supra* note 75, at 7.
[79] *See generally* Toohey, *supra* note 27, at 31-33.
[80] *See* Emma Witman, *What Is Metadata? Understanding the Types of Data That Describes Data Sets and Determines Much of What You See Online*, BUS. INSIDER: REVS. (Jun. 17, 2021, 11:54 AM), https://www.businessinsider.com/guides/tech/what-is-metadata.
[81] Ratnaswamy, *supra* note 28, at 43.
[82] Kinsey, *supra* note 60.
[83] *Id.*
[84] Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata*, 113 PROCS. NAT'L ACAD. SCIS. U.S. AM. 5536, 5540 (2014).

and often know little about cyber security practices. The legal profession has a strong history of traditionalism, which sometimes means pushback on technological focus.[85] Not only have certain technological issues not been addressed, but some lawyers may not even be fully aware of these problems and how they pertain to their confidentiality obligations.[86] The legal profession has generally not invested many resources into dealing with these potential issues. Law firms tend to spend less money on cyber security experts compared to companies of similar size in other industries; they are often reluctant to spend time and money on data protection despite the growing threats.[87] Law firms often do not utilize the same security processes that are expected of large corporations in other industries, leaving law firms especially vulnerable.[88] Moreover, certain cyber-attacks can be difficult to detect, and thus, leaves people being unaware that their data has been exposed. A 2013 report found that 65% of cyber espionage attacks took months to detect.[89] In 2020, many lawyers reported they had experienced a breach, and many others were unaware of whether or not a breach had occurred.[90] This exemplifies how vulnerable many law firms are to cyber-attacks. Also, in 2020, more than half of all lawyers were not using any kind of email encryption or file encryption.[91] This means that in the event of any kind of breach, the information in those emails or files would be easily readable and available to anyone who gained access to them. In light of this data, it is clear that law firms are not as secure as they could be.

The lack of security protocols and an unwillingness to utilize security technology is concerning because law firms are increasingly being targeted by cyber-attacks.[92] Law firms are prime targets for ransomware due to the large amount of sensitive information they store.[93] Even law firms that are considered technologically savvy and are more aware of these problems are still at risk.[94]

Many legal communications, including ones that possess confidential information, take place via electronic communications. The increased use of electronic devices can cause different issues, depending on the nature of the device and the precautions taken. The increased use of cellphones as a primary method of communication can potentially cause breaches, as both digital and analog phone conversations can be intercepted.[95] Even if a lawyer is careful to only use methods of communication that they know to be secure, it is likely that the client will be less careful and privileged conversations may be vulnerable.[96]

---

[85] Toohey, *supra* note 27, at 1-2; 4-6.
[86] *Id.*
[87] Conte, *supra* note 32.
[88] *Id.*
[89] Toohey, *supra* note 27, at 7-8.
[90] John Loughnane, *2020 Cybersecurity*, AM. BAR ASS'N (Oct. 19, 2020), https://www.americanbar.org/groups/law_practice/resources/tech-report/archive/cybersecurity/.
[91] *Id.*
[92] AJ Shankar, *Ransomware Attackers Take Aim at Law Firms*, FORBES (Mar. 12, 2021, 8:50 AM), https://www.forbes.com/sites/forbestechcouncil/2021/03/12/ransomware-attackers-take-aim-at-law-firms/?sh=335060daa13e.
[93] *Id.*
[94] Daniel W. Hagar, *Enhanced Cybersecurity Is Imperative for Arizona Lawyers*, ATT'Y L. MAG. (June 20, 2019), https://attorneyatlawmagazine.com/legal-vendors/insurance/enhanced-cybersecurity-imperative-arizona-lawyers.
[95] David J Bilinsky & Laura Calloway, *Lawyers, Cell Phones, Ethics, and Security*, 20 SEC. & ETHICS 34, 36 (2003).
[96] *Id.*

Therefore, lawyers must always consider the potential vulnerabilities associated with shared information.

There are even more risks associated with communications that occur electronically, especially over the Internet. A large number of corporate communications, including communications related to legal business, now occur over email, connecting these conversations and the information associated with them to the Internet.[97] Tablets and other forms of portable computers can cause privacy breaches, especially now that these devices are increasingly used for legal work.[98] These devices are frequently lost or misplaced, making any data stored on them vulnerable.[99] Data is often unnecessarily left available and vulnerable on devices that lawyers use to work remotely; less than half of all lawyers in 2020 used any kind of remote device management or wiping tool.[100]

c. Current Guidelines

The American Bar Association has made decisions regarding emerging technology, often attempting to use the Model Rules to deal with these changes.[101] However, this has only occurred in a limited fashion, and there are still issues that have not been addressed. Additionally, every state bar has not followed the recommendations given by the ABA, and many of these guidelines are in comments and other non-authoritative recommendations.[102] In 1999, it was determined by the American Bar Association that it is acceptable to use email for legal communications and to send confidential information via email because the Internet offers a sufficient degree of privacy compared to the methods of communication used by lawyers in the past.[103] However, it can be argued that times have changed significantly since the years in which these decisions were made. Questions have arisen regarding the safety of email and there has been increasing concern about cyber security attacks and the ways electronic communications could be intercepted.

Metadata is a bigger concern now than it was in the past because an increasing amount of information may be transmitted that the sender may not be aware of or intend to transmit. This decision was made because email has a similar level of privacy to phone calls via landline and physical mail via the post office.[104] However, this does not take into account how easy it is to transmit an email to another person.[105] A phone call cannot be mass-shared in the way that an email can.[106] In the event of a breach, email messages are much more likely to be stored and therefore vulnerable to being leaked.[107] This means emails carry many risks that other forms of communication may not have. But, a 2010 opinion

[97] Toohey, *supra* note 27, at 2.
[98] Bilinsky, *supra* note 95, at 38.
[99] *Id.*
[100] Loughnane, *supra* note 90.
[101] *See A Re-Examination of the ABA Model Rules of Professional Conduct Pertaining to Client Development in Light of Emerging Technologies*, AM. BAR, https://www.americanbar.org/groups/professional_responsibility/resources/professionalism/professionalism_ethics_in_lawyer_advertising/ethicswhitepaper/ (last accessed Apr. 20, 2024).
[102] MODEL RULES OF PRO. CONDUCT Preamble & Scope (AM. BAR ASS'N 1983).
[103] McEnroe, *supra* note 59, at 191.
[104] Toohey, *supra* note 27, at 23.
[105] *Id.*
[106] *Id.*
[107] *Id.*

by the American Bar Association stated that it is acceptable to utilize a personal wireless system for communications as long as the system has "appropriate security features," which may include encryption and firewalls.[108] However, it is important to highlight that the opinion warns about utilizing public wireless communication systems because they typically lack these security features.[109]

In 2009, the ABA discussed how the Model Rules apply to emerging technology and addressed some issues associated with these technologies.[110] At this time, an important change was made to Model Rule 1.1, which addresses the competency requirements for lawyers; in order to be considered competent under the model rules, lawyers are now required to keep up to date regarding "the benefits and risks associated with relevant technologies."[111] This could mean that a lawyer could potentially be accused of violating professional ethics for failing to be aware of the potential harm associated with the technology they are using. However, it is unclear exactly how knowledgeable lawyers must be to satisfy their competency requirements, especially regarding the quickly evolving field of technology. Generally, lawyers must only have a "reasonable" amount of knowledge regarding current technology.[112] Different people and different jurisdictions will have widely varying ideas about what a reasonable amount of knowledge is. Therefore, it is unclear how much technology training a lawyer must go through to continue practicing.

In 2012, the American Bar Association added a comment to Model Rule 1.6(c).[113] This comment "requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision."[114] Competently safeguarding information could include putting precautions in place to prevent unauthorized persons from gaining access to information electronically, which could lead to enacting cyber security protections. Whether a lawyer's attempts to protect the information will be considered reasonably sufficient depends on a number of factors, including "sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients."[115] There is significant leeway for lawyers in the actions they take to protect data, especially since there are allowances made for safeguards that would be difficult or costly to implement. Regulations regarding data tend to be reactive. Many problems will not be addressed until harm comes as a result of the lack of regulation. Even with harm occurring and privacy being clearly at risk, the legal profession has been slow to react.[116]

---

[108] *Id.* at 20.
[109] *Id.*
[110] James Podgers, *The Fundamentals: Lawyers Struggle to Reconcile New Technology with Traditional Ethics Rules*, 100 ABA J. 22, 22 (2014).
[111] MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 1983).
[112] Podgers, *supra* note 110, at 23.
[113] MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 1983).
[114] *Id.*
[115] *Id.*
[116] *See* Borden, *supra* note 46, at 1-8.

There are regulations that may potentially apply to lawyers and law firms, depending on the State they operate in. Some of these issues have been addressed to some extent by the bars of individual states. Recently, the Arizona State Bar published an ethics decision regarding metadata.[117] This decision prohibits lawyers from mining metadata, as well as requiring legal professionals to scrub metadata from any confidential documents electronically sent.[118] Mining metadata means "searching for metadata using software applications that are designed to retrieve metadata despite a sending lawyer's reasonable efforts to scrub it."[119]

In most states, there are obligations involving data security that apply to all businesses. In forty-eight states, there are laws requiring that in the event of a security breach, any business must inform those who may have had their information accessed.[120] A few states, such as California, have more requirements, including that businesses—including law firms—must "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use modification, or disclosure."[121]

While the privacy issues caused by more recent technology are something that has been addressed by some authoritative bodies, awareness is still lacking in the legal profession. These issues are not being properly dealt with, and most of the available guidelines are vague or overly lenient regarding the obligations of legal professionals. This leaves legal data and confidential communications to significant risk.

III. Recommendations

It is important for the legal profession to consider the problems resulting from current and future technology, especially when this technology becomes an integral part of the industry and of everyday life. The legal profession must especially be aware of how technology is impacting the obligations that lawyers have in protecting privacy. In order for a lawyer to be considered competent enough to practice under MRPC 1.1, it is the responsibility of lawyers to weigh the benefits of using certain technologies against the harms that may occur as a result of using them.[122] The usage of some newer technology cannot be avoided. In these cases, lawyers should be aware of the potential risks and the ways in which these technologies may impact privacy.[123] Legal professionals are not the only ones who must contend with the ways in which technology has caused problems regarding privacy ethics. The legal profession should self-regulate their technology in a way similar to other industries that must deal with sensitive information, such as the medical and banking industries.[124] Moreover, the legal profession must enact more and stricter guidelines regarding technology. Client data should be kept as safe as possible, which means that the legal profession must do whatever it can to regulate the safety of

[117] Bradley Perry, *Metadata: Landmine or Buried Treasure?*, ARIZ. ATT'Y MAG., Oct. 2022, at 10; *see generally* Witman, *supra* note 70.
[118] *Id.*
[119] Ariz. Att'y Ethics Advisory Comm., Op. EO-20-0008 (2022).
[120] Toohey, *supra* note 27, at 14.
[121] *Id.* at 23.
[122] *See* MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 1983).
[123] *See* McEnroe, *supra* note 59, at 192-94.
[124] Kenneth N. Rashbaum et al., *Cybersecurity: Business Imperative for Law Firms; Outside Counsel*, N.Y. L. J. (2014), https://plus.lexis.com/api/permalink/1d9852d7-230c-4c4c-b95f-1e7fecea8ec4/?context=1530671.

legal information. Otherwise, the profession's reputation will suffer and people will be less likely to trust their lawyers.[125]

a. Data Protection Procedures

Lawyers need to be up to date on cyber security. They must be aware of current risks and take precautions to protect data. It is already recommended by the American Bar Association they implement "reasonable" safeguards[126]- a lawyer should consider what these safeguards may be and be willing to potentially spend time and money implementing them. Lawyers must also understand the amount of information they are potentially sharing at all times. This is especially important when considering metadata; a lawyer must understand metadata well enough to avoid sharing information that they should not be.[127] New technology may often have complicated implications that may not be easily foreseen, especially by someone who does not have a good understanding of that technology.[128] Lawyers must remember to analyze the technological advancements impacting their legal work, which may require an increased level of technological knowledge.

Lawyers should be expected to utilize technology that would keep their data more secure. Lawyers who are storing or transmitting data electronically should use some form of encryption. Encryption is a way of encoding data so that it cannot be accessed or altered by someone who has not been given the ability to do so.[129] Encryption is used by too few lawyers, which means that confidential legal data will be easy to read if it is accessed by a third party.[130] Encrypting files is a safeguard that would make it more difficult for a malicious actor to access data, albeit it is possible for a malicious actor to de-encrypt files. Encryption would also prevent someone who received the email by accident from easily reading sensitive information.[131] Ultimately, encryption is a basic and typically inexpensive piece of technology that may make it more difficult for unknown parties to access a law firm's sensitive data, thus decreasing both the chances of a privacy breach, as well as decreasing the potential harm done by a breach.[132] Therefore, using encryption should be considered a "reasonable" security precaution.[133]

Client data should only be used for the client's legal representation. After someone is no longer a client, it may be best if their data is not saved. If the past client's data is not saved, then the data would no longer be vulnerable to privacy breaches and the amount of data a lawyer is responsible to protect would decrease. If a data breach does occur, less sensitive information will be available to hackers, which decreases the amount of potential harm. Law firms should consider what information is really necessary and whether it is worth the risk to keep. Part of the reason why certain technologies are regarded as safe is because it was previously assumed that any sensitive information

[125] Matich, *supra* note 50.
[126] MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 1983).
[127] Mayer, *supra* note 84, at 5536.
[128] Borden, *supra* note 46, at 7-8.
[129] Box Communications, *What Is File Encryption?*, BOX BLOGS (Oct. 28, 2021), https://blog.box.com/what-is-file-encryption.
[130] Loughnane, *supra* note 90.
[131] Box Communications, *supra* note 129.
[132] *See* Matich, *supra* note 50.
[133] *See* MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 1983).

would end up being deleted relatively quickly.[134] This was especially true in the 1990s, when many opinions about technology were being formed and the American Bar Association's decision regarding email was made.[135] At this time, storage space was more expensive, which meant that data was not kept as long.[136] Email providers during this time period, such as AOL, would delete emails from their servers after only a matter of days.[137] This has changed significantly in recent years.[138] Now, digital storage space is cheap, and it is easy to keep huge quantities of data saved indefinitely.[139] Not only are many companies able to keep data over prolonged periods, but someone may not even be aware of the data still being saved because a backup of any file could exist on Internet web servers, such as those used by Google and Microsoft.[140] Lawyers should stay aware of the data-saving policies of any communication or data storage product that they are using, especially if it is saving data to a cloud; otherwise they may not be fully aware of how long that data will exist or who might be able to gain access to it. Lawyers should have policies regarding how much data they will save and for how long. Additionally, they should be aware of any related policies in the products or services that they are using.

Currently, the only rules regarding technology in the ABA's Model Rules focus on efforts that individual lawyers should make when protecting confidential information and when learning to use new technology.[141] These rules are not very specific about what those efforts should be.[142] For the legal profession to deal with certain issues, there must be more requirements that force legal professionals to take more specific precautions. Lawyers should also be adjusted as new technology is invented, as well as when the current technology changes; one cannot rely on old statements that were made before several modern-day innovations. These changes should include stricter and more detailed rules for law firms and legal professionals. It is important for there to be improved rules for law firms. Law firms must be willing to invest more time and money into cyber security precautions. Currently, law firms invest very little in cyber security, making the legal profession especially vulnerable.[143] Law firms are already an enticing target for hackers due to the amount of sensitive information they commonly have stored, and because law firms have less cyber security than similar businesses they are even more attractive for hackers to target.[144] Legal professionals must become more prepared to safeguard against cyber-attacks and to deal with them if they do happen; this may require regulatory bodies to step in and ensure that these precautions are taken. However, it would be best if the legal profession can properly self-regulate with these issues as it does for other issues.[145]

b. Increasing Technological Knowledge

Law firms should ensure that their employed are knowledgeable enough about technology

[134] Toohey, *supra* note 27, at 24.
[135] *Id.* at 24-25.
[136] *Id.* at 24.
[137] *Id.*
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *See generally* MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 1983).
[142] *See generally id.*
[143] Conte, *supra* note 32.
[144] *Id.*
[145] *See generally*, Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817, 859-66 (2012).

to be able to take reasonable precautions to protect client privacy. In many jurisdictions, awareness about technology is no longer optional, as the Model Rules of Professional Conduct consider being knowledgeable about current relevant technology to be a requirement for competency in lawyers.[146] This is a fairly broad requirement, but many jurisdictions have additional, more specific rules that lawyers must be aware of.[147] For example, in Arizona, it is required that lawyers remove any confidential metadata from the documents they send to people other than their clients.[148] This means that these lawyers must have some degree of technological knowledge and understanding of what metadata is.[149] There must be more focus on training lawyers to be knowledgeable about technology to avoid mistakes, especially mistakes that may lead to breaches of privacy.[150] Law firms should be prepared to train their employees about technology in general and in any technology used by the firm. They must also be prepared to alter their protocols and training procedures when they implement new technology or when the technology that they are already using undergoes any significant changes.

Lawyers are already required to undergo certain training to begin and to continue practicing. In most states, lawyers are required to take continuing legal education classes to continue practicing law. In Arizona, fifteen hours of continuing legal education are required; three of these hours must have a focus on ethics.[151] A lawyer's continuing legal education should include classes focusing on how to properly use emerging technologies and about issues that might arise from using this technology. Rather than increase the overall number of hours required for continuing legal education, the number of hours can remain the same, but some of those hours should be spent learning about technological issues in the legal profession like, how three hours are already required to be focused on ethics.[152] The tech-based classes for lawyers could include education about cyber security, information ethics, metadata, and new technology that may be relevant in legal practice. Some of these topics are already discussed in Continuing Legal Education classes.[153] For example, one Continuing Legal Education class available to legal professionals in Arizona is titled "Preventing Your Worst Tech Nightmare: Protecting Your Firm and Clients from Cybercriminals."[154] This course is meant to educate legal professionals about cyber security and teach different ways that one might protect their confidential information against cyber-attacks.[155] This is an example of the type of class that should be made mandatory. For this initiative to be successful, it would also be important to increase the number of Continuing Legal Education classes available that are related to technological issues. There should not only be classes about cyber security, but there should also be classes about the ethical usage of any new technology that becomes a part of the legal profession.

---

[146] MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 1983).
[147] *See, e.g.*, Perry, *supra* note 117.
[148] *Id.*
[149] *Id.*
[150] Toohey, *supra* note 27, at 21-22.
[151] *Arizona CLE Requirements and Courses*, AM. BAR ASS'N, https://www.americanbar.org/events-cle/mcle/jurisdiction/arizona/ (last visited Feb. 17, 2024).
[152] *Id.*
[153] *E.g.*, *Preventing Your Worst Tech Nightmare: Protecting Your Firm and Clients from Cybercriminals*, NAT'L ACAD. CONTINUING LEGAL EDUC., https://www.nacle.com/CLE/Courses/Preventing-Your-Worst-Tech-Nightmare-Protecting-Your-Firm-and-Clients-from-Cyber-2156 (last visited Feb. 17, 2024).
[154] *Id.*
[155] *Id.*

Additionally, law firms should also be involved in keeping the legal profession informed about technological issues. Law firms should ensure that all of the lawyers they hire are properly trained and knowledgeable about any technology that they may be using or involved with. Lawyers should be trained on how they are expected to deal with emails. This could include ensuring that any emails are sent to the correct person and that the email, as well as any files sent with it, do not contain sensitive metadata. Lawyers should also be taught how to receive emails. A lawyer clicking on a link or submitting information to a fraudulent email can cause a lot of security problems for a law firm.[156] Lawyers should be trained on how to spot fraudulent emails, and it may be best for them to act proactively even if they only have a slight suspicion about an email. Lawyers should send any potentially fraudulent emails along to the law firm's IT department.[157] Every law firm must have a consistent protocol for emails. Law firms must especially plan for how to identify and deal with fraudulent emails. This may involve both training their employees to follow specific practices, as well as ensuring that they have a robust IT department that is aware of cyber security threats and can deal with them appropriately.

c. Tightening Existing Guidelines

Law firms must also be prepared to invest more into cyber security. The legal profession should be spending just as much time and money on cyber security as other industries. In fact, they may need to spend more because law firms have been so frequently targeted and it is especially crucial that legal information be kept private. While it may be costly, it will be worth it in the long run due to how costly a cyber-attack can be.[158] Additionally, doing everything possible to protect clients' privacy should be considered an ethical and professional obligation for all legal professionals. In one survey, it was found that 25% of all law firms experienced a cyber security breach in 2021.[159] This is far too high a number for the legal profession to ignore. While proper security measures can be expensive, the harm caused by cyber security attacks can be far more costly.[160] Even when proper precautions are in place, law firms also need to be prepared for how they will address a cyber security breach if one does occur. Many law firms would benefit from looking into their insurance coverage for cyber security, which is not always covered by more general insurance packages.[161] Choosing a cyber security insurance package requires law firms to perform research and consider where there might be flaws in their security.[162] Law firms must spend more resources understanding the technology it uses and the problems that may arise from those technologies.

The legal profession should follow in the footsteps of other industries when it comes to electronic privacy. Other industries that deal with protected information are highly regulated. The medical industry is a good example to follow because medical information is also very sensitive, and medical professionals are meant to have a code of professional ethics regarding privacy.[163] In their code of professional ethics, medical professionals

[156] *See* Roberta Tepper, *Not Being Scammed*, ARIZ. ATT'Y MAG., Apr. 2021, at 10, 10.
[157] *Id.*
[158] Kate Myers, *"Affirmative" and "Silent" Cyber Insurance Protecting Your Firm in 2022*, ARIZ. ATT'Y MAG., Oct. 2022, at 42, 42.
[159] *Id.*
[160] *See id.*
[161] *Id.* at 44, 46.
[162] *Id.* at 44-46.
[163] *See infra* notes 158, 161.

have similar obligations regarding confidentiality.[164] Like a lawyer's client, a patient expects the information they give to a medical professional to be kept private.[165] However, the medical industry differs from the legal profession in that there are more specific regulations regarding how this information is kept secure, and some of these regulations are enforced by the federal government.[166] This includes guidelines for storing and securing electronic records.[167] Medical professionals are required to form a consistent system regarding medical records; this system must "conform to acceptable industry practices and standards."[168] Medical ethics also require that "measures to ensure data security and integrity" must be included in their information security system.[169] Additionally, the Code of Medical Ethics gives specific instructions for dealing with a security breach if one does occur, which requires disclosing the breach to all relevant parties and taking steps to mitigate the harm done by the breach.[170] There are further legal consequences for medical professionals who fail to protect the privacy of their patients.[171] This is included in the Health Insurance Portability and Accountability Act (HIPAA), a federal law that regulates healthcare professionals and creates obligations for them to protect medical records.[172] HIPAA has specifications regarding electronically protected health information, which includes an obligation to "detect and safeguard against anticipated threats to the security of the information."[173] This implies an obligation to be aware of cyber security issues, as well as proper protocol for securing digital information.[174] Medical professionals cannot ignore technological threats to privacy like legal professionals can, or they may face more severe legal ramifications.[175] Like the medical industry, the legal profession should further codify requirements regarding cyber security and privacy breaches. The legal profession should also have more guidelines regarding digital information and could potentially use the medical industry as a template for these guidelines.

The banking industry is another potential example of how to handle privacy. The federal government primarily regulates privacy through the Federal Deposit Insurance Corporation (FDIC) and the Federal Trade Commission (FTC).[176] The FDIC handbook

---

[164] *See Privacy, Confidentiality & Medical Records*, AMA CODE MED. ETHICS, https://www.ama-assn.org/delivering-care/ethics/code-medical-ethics-privacy-confidentiality-medical-records (last visited Feb. 17, 2024).
[165] *See id.*
[166] *See generally Summary of the HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last updated Oct. 19, 2022).
[167] *Confidentiality & Electronic Medical Records*, AMA CODE MED. ETHICS, https://www.ama-assn.org/delivering-care/ethics/confidentiality-electronic-medical-records (last visited Apr. 20, 2024).
[168] *Id.*
[169] *Id.*
[170] *Breach of Security in Electronic Medical Records*, AMA CODE MED. ETHICS, https://www.ama-assn.org/delivering-care/ethics/breach-security-electronic-medical-records (last visited Apr. 20, 2024).
[171] *Id.*
[172] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL & PREVENTION https://www.cdc.gov/phlp/publications/topic/hipaa.html (last updated June 27, 2022).
[173] *Id.*
[174] *See Id.*
[175] *See HIPAA Violations & Enforcement*, AMA, https://www.ama-assn.org/practice-management/hipaa/hipaa-violations-enforcement/ (last accessed Apr. 20, 2024).
[176] *See Privacy Rule Handbook*, FDIC, https://www.fdic.gov/regulations/examinations/financialprivacy/handbook/ (last updated Nov. 8, 2023); *Protecting Consumers' Financial Privacy*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/financial-privacy (last visited Apr. 20, 2024).

describes several regulations regarding how to protect banking customers' privacy.[177] Agencies are expected to take certain steps to secure data.[178] The FTC has specific guidelines regarding how to keep private data secure.[179] A financial institution must create an information security program, and is expected to "identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information."[180] There are guidelines in the banking industry that the legal profession could utilize. In particular, the FTC gives very specific regulations regarding cyber security and other technological threats to privacy, while similar rules in the legal profession are much broader.[181] If the legal profession had more specific rules like the banking industry has, there would be much more standardization in how information is protected.

The legal profession could benefit from taking some of the precautions other industries have taken. The medical and banking industries in particular are good examples because these industries also deal with a lot of very sensitive information and are expected to be heavily regulated due to the severe consequences that can occur if this information is leaked.[182] The legal profession currently has many of the same expectations regarding privacy as these other industries do, as well as a similar overall set of professional values, but the legal profession has not always fulfilled these expectations or upheld these values successfully.[183] This is partially due to the fewer rules committed to dealing with new privacy issues.[184]

There are certain ways the legal profession is unique which means they probably cannot be regulated the same way these other industries are. The medical and banking industries are regulated significantly by the government.[185] However, the legal profession regulates itself;[186] thus, people cannot rely on government standards when seeking legal help but must instead trust the standards of the profession. Despite the different hierarchies of authority present in the legal profession, there are still elements from other industries that could be applicable.

The legal profession should enact stricter rules regarding the use of technology and how it pertains to privacy. The idea of tightening guidelines surrounding information issues

[177] *Privacy Rule Handbook, supra* note 176.
[178] *Id.*
[179] Standards for Safeguarding Customer Information, 86 Fed. Reg. 70272, 70272 (Dec. 9, 2021) (to be codified at 16 C.F.R. pt. 314), https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information.
[180] *Id.*
[181] *See, e.g.*, *FTC Extends Deadline by Six Months for Compliance with Some Changes to Financial Data Security Rule*, FED. TRADE COMM'N (Nov. 15, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/11/ftc-extends-deadline-six-months-compliance-some-changes-financial-data-security-rule; *ABA Urges Lawyers to Raise their Cybersecurity Game,* ESQUIRE DEPOSITION SOLUTIONS (Aug. 10, 2023), https://www.esquiresolutions.com/aba-urges-lawyers-to-raise-their-cybersecurity-game/.
[182] *See Breach of Security in Electronic Medical Records, supra* note 170; *Privacy Rule Handbook, supra* note 176.
[183] *See* Asokan, *supra* note 1; Mühlberg, *supra* note 7; Toohey, *supra* note 27, at 3-4, 45-47.
[184] *See generally* MODEL RULES OF PRO. CONDUCT (AM. BAR ASS'N 1983).
[185] *See Breach of Security in Electronic Medical Records, supra* note 170; *Privacy Rule Handbook, supra* note 176.
[186] MODEL RULES OF PRO. CONDUCT Preamble & Scope (AM. BAR ASS'N 1983).

will not be new to the profession.[187] The American Bar Association has already enacted detailed ethical obligations connected to confidentiality.[188] For example, keeping client information confidential is not an absolute obligation; several exceptions are fairly specific.[189] More rules could have this level of detail, especially when pertaining to a lawyer's technological obligations and level of required knowledge. The American Bar Association must also prepare to enforce these rules. There is already a structure for enforcing legal ethics and potentially punishing those in breach.[190] There should be potential for suspension for those not taking appropriate steps to protect confidential information, as this issue can cause significant harm if the person is allowed to continue practicing in this unsafe fashion.

The legal profession must act on these privacy issues as soon as possible. It must also be ready to deal with new issues arising from continually advancing technology. There are several possible negative consequences if the legal profession does not take steps to adjust to modern technology.[191] A perceived lack of privacy tends to make people more reluctant to speak about certain things.[192] If clients believe that their sensitive information may not be safe, they may be less likely to share information with their lawyers, even if this information is crucial to their legal proceedings. This will limit how much a lawyer is able to help them. The previous pattern of reactive regulation is not sufficient. The legal profession cannot wait until a crisis happens before it will change; it must instead take preventative measures as soon as possible. A privacy breach can cause significant damage. For example, a law firm's data being leaked could mean that all of their clients have now had sensitive information made more public. Moreover, this would have a severe impact on the reputation of both the law firm and of the noble legal profession.

IV. Conclusion

Modern technology is not something that the legal profession can avoid; the problematic implications these technologies have for privacy also cannot be avoided but can be ameliorated. Legal professionals must be prepared to deal with the potential ethical consequences of using this technology. Information is increasingly vulnerable, making privacy ethics more important than ever. Lawyers especially have an obligation to be concerned with privacy due to their professional responsibilities regarding confidentiality. Professional conduct in the legal profession must be adjusted in order to reflect the changing technological landscape. These changes would include a variety of approaches, including more comprehensive education about technological issues and more specific guidelines.

REvil's attack on Grubman Shire Meiselas and Sacks could have been prevented if the firm had kept more up-to-date about recent cyber security threats and were more aware of possible vulnerabilities in their data protection plan. If the firm had taken more precautions, then the massive amount of leaked data would have likely been protected.

---

[187] *Data Privacy Principles All Legal Providers Should Adopt*, THOMSON REUTERS, https://legal.thomsonreuters.com/en/insights/articles/data-privacy-principles (last accessed Apr. 20, 2024).
[188] *E.g.*, MODEL RULES OF PRO. CONDUCT r. 1.6(b) (AM. BAR ASS'N 1983).
[189] *Id.*
[190] *Id.* at r. 8 (AM. BAR ASS'N 1983).
[191] Matich, *supra* note 50.
[192] *See* Magi, *supra* note 20, at 188.

Legal professionals have the potential to prevent ethical crises before they happen by increasing awareness of technological threats to privacy and by increasing regulations surrounding how technology is used by the industry. The legal profession must act now rather than wait to respond.