Legal Ethics' Next Frontier: Lawyers and Cybersecurity

*Eli Wald**

The publication of the Panama Papers containing confidential client information, following a cybersecurity breach at the law firm of Mossack Fonseca, demonstrated what many have long known, that law firms are particularly vulnerable to cyberattacks.[1] Yet since concerns about law firms' cyber practices have first surfaced, the legal profession has learned a lot about cybersecurity. We know who is perpetrating cyberattacks against lawyers, we know why they are doing it, and we even know quite a bit about how to prevent and defend against attacks, as well as how to mitigate their damage and respond when an attack takes place. Still, there are quite a few things we do not know. Most importantly, we do not know the extent and scope of cyberattacks against law firms, and we do not know whether lawyers are acting on the growing body of cybersecurity knowledge they possess to reasonably protect their clients' information from unauthorized access. Indeed, we have reason to believe that some

* Charles W. Delaney Jr. Professor of Law, University of Denver Sturm College of Law. I thank Denis Binder, Tanya Forsheit, Scott Garner, Marty Katz, Ron Rotunda, Drew Simshaw, and other participants in the "Cyber Wars: Navigating Responsibilities for the Public and Private Sector" Symposium at Chapman University Dale E. Fowler School of Law for their helpful comments. I also thank Diane Burkhardt, Faculty Services Liaison at the Westminster Law Library at the University of Denver Sturm College of Law, for her outstanding research assistance.

1 On the Panama Papers, see Luke Harding, *What Are the Panama Papers? A Guide to History's Biggest Data Leak*, GUARDIAN (Apr. 5, 2016), http://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers [http://perma.cc/PG79-Z7HM]; David Z. Morris, *The Laughably Bad Security at 'Panama Papers' firm Mossack Fonseca*, FORTUNE (Apr. 9, 2016), http://fortune.com/2016/04/09/bad-security-panama-papers/ [http://perma.cc/453A-ZXZB]. The Federal Bureau of Investigation publicly identified law firms as vulnerable in 2009, see Susan Hansen, *Cyber Attacks Upend Attorney-Client Privilege*, BLOOMBERG (Mar. 19, 2015, 11:56 AM), http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security [http://perma.cc/8LSR-5UEQ]. The FBI reiterated its caution in 2011, calling on major law firms to raise their level of awareness regarding cyberattacks. *See* Anne Marie Davine, *More Cyber Preparedness Needed, According to 2014 Law Firm Cyber Survey*, MARSH (Jan. 15, 2015), https://www.marsh.com/us/insights/more-cyber-preparedness-needed-2014-law-firm-cyber-survey.html [http://perma.cc/5SFK-TTQ9]. FBI officials and security experts maintain that law firms remain a weak link when it comes to online security. *Id.*

lawyers, notwithstanding their awareness of cybersecurity threats, fail to take reasonable steps to protect themselves and their clients, because they are underregulated, likely to escape any meaningful consequences for their inaction, and therefore, have little incentive to take reasonable cybersecurity action.

Lawyers' cybersecurity conduct is underregulated because the usual regulatory suspects, liability rules and market controls, do not rigorously apply. Since proving cybersecurity damages is often hard to do, lawyers do not systematically face the prospect of malpractice liability for failing to adequately protect clients' information. Since lawyers are generally under no duty to report cyberattacks to their clients or to others, they do not face market sanctions, such as being fired or suffering reputational losses. Of course, some lawyers have been at the forefront of practicing diligent cybersecurity. Yet, because practicing cybersecurity is expensive and the technological learning curve for lawyers is steep, in the face of underregulation and few practical consequences for inaction, some lawyers may fail to reasonably defend against cyberthreats, the known risks notwithstanding.[2] Moreover, because malpractice lawsuits are scarce, there is little in the way of judicial exposition of the meaning of *reasonable* cybersecurity practices, leaving even those lawyers who are committed to practicing reasonable cybersecurity in the dark.

This Article argues that the underregulation of lawyers' cybersecurity conduct may be addressed by the promulgation of robust rules of professional conduct, delineating the meaning of reasonable cybersecurity protections and mandating greater disclosure of unauthorized access to clients. Effective rules of professional conduct are likely to incentivize lawyers to take action for three related reasons. First, the threat of discipline will motivate some lawyers to take reasonable cybersecurity action and advise clients when attacks result in compromised information. Second, a mandatory disclosure duty will in turn enable more effective market regulation as clients will be able to sanction lawyers for inaction. Third, the promulgation of effective cybersecurity rules may result in peer pressure and the development of reasonable cybersecurity social norms among lawyers.

Part I of the Article summarizes the knowledge lawyers have recently gained about cybersecurity, namely, who is attacking them, why, and what can be done to defend against cyberattacks.

---

2 James R. Silkenat, *Privacy and Data Security for Lawyers*, 38 AM. J. TRIAL ADVOC. 449, 454 (2015) ("[B]ut in the case of cybersecurity, attorneys sometimes take a more 'do as I say, not as I do' approach.").

Part II examines the underregulation of lawyers' cybersecurity conduct and its consequences. Part III advances a proposal for a regulatory response, in the form of new and revised rules of professional conduct.

I. THE STATE OF LAWYERS' CYBERSECURITY KNOWLEDGE

The use of technology is pervasive in the practice of law. Like many other professions, lawyers e-mail, store information remotely, share files, and use mobile devices and wireless networks; their "widespread use of electronic records and mobile devices" presents "unprecedented challenges."[3] As *The ABA Cybersecurity Handbook* explains, "[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 or destruction."[4] Lawyers must understand and respond to these risks in order to protect confidential client information, which if compromised, can expose clients to the loss of the attorney-client privilege, fraud, negative publicity and tarnished business reputations, liability to others, and even bankruptcy.[5]

Over the last few years, however, the legal profession has learned a great deal about cybersecurity. Lawyers now know why they have become likely targets for hackers, who is perpetrating the attacks, and what they can do to minimize the probability and severity of attacks before they take place, as well as respond to attacks when they happen. This part briefly summarizes the growing wealth of information about cybersecurity.

A. Why Lawyers Are Under (Cyber) Attack

Lawyers experience cyberattacks for three related reasons: they store valuable confidential client information, they are likely to be more vulnerable than their clients, and they are under increased pressure to take advantage of technologies that render them susceptible to attacks. To begin with, cybersecurity is traditionally concerned with protecting confidential information,

---

3 ABA CYBERSECURITY LEGAL TASK FORCE & SECTION OF SCIENCE & TECHNOLOGY LAW, REPORT TO THE HOUSE OF DELEGATES: RESOLUTION 109, ABA 4 (Aug. 2014) [hereinafter ABA CYBERSECURITY RESOLUTION], http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2014_hod_annual_meeting_109.authcheckdam.pdf [http://perma.cc/NS7C-JXS7].

4 JILL D. RHODES & VINCENT I. POLLEY, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS 41 (2013). *See generally* MARC GOODMAN, FUTURE CRIMES – EVERYTHING IS CONNECTED, EVERYONE IS VULNERABLE, AND WHAT WE CAN DO ABOUT IT (2015).

5 Drew T. Simshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data*, 38 AM. J. TRIAL ADVOC. 549, 550, 554 (2015).

maintaining the integrity of information, and ensuring the availability of stored information.[6] Protecting confidential information is especially important to the legal profession, as all lawyers and law firms are depositories of valuable confidential information related to the representation of clients. As the American Bar Association Model Rules of Professional Conduct ("Rules") explain, protecting confidential information is a "fundamental principle" that "contributes to the trust that is the hallmark of the client-lawyer relationship."[7] Confidentiality encourages clients "to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively."[8] Put differently, to effectively represent clients, lawyers routinely collect and store valuable client information. Because lawyers receive and store valuable confidential information pertaining to their clients' matters, they are likely targets for hackers.

Context always matters in the practice of law,[9] and it is essential to gaining an understanding of the cybersecurity practices of lawyers. Different types of law firms offer different types of potential value to hackers in terms of the confidential client information they store. For example, hacking large law firms, which tend to represent large entity clients,[10] is often more

---

6 David G. Delaney, *Cybersecurity and the Administrative National Security State: Framing the Issues for Federal Legislation*, 40 J. LEGIS. 251, 251 (2014) ("At its core, cybersecurity involves information security or assurance—preserving the confidentiality, availability, and integrity of information."). The core objectives of confidentiality, availability, and integrity of information inform cybersecurity legislation. For example, under the Health Insurance Portability and Accountability Act, covered entities "must assure their customers (for example, patients, insured individuals, providers, and health plans) that the integrity, confidentiality, and availability of electronic protected health information they collect, maintain, use, or transmit is protected." *See* Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003). Similarly, the National Institute of Standards and Technology ("NIST"), a Department of Commerce non-regulatory agency, "provide[s] standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services." *See Computer Security Resource Center*, NIST, http://www.nist.gov/itl/csd/csrc.cfm [http://perma.cc/K7RV-XMPR] (last updated Oct. 5, 2010).

7 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 2 (AM. BAR ASS'N 2013).

8 *Id.*

9 Eli Wald, *Resizing the Rules of Professional Conduct*, 27 GEO. J. LEGAL ETHICS 227, 235–44 (2014); David B. Wilkins, *Legal Realism for Lawyers*, 104 HARV. L. REV. 468, 473, 476, 515–19 (1990); David B. Wilkins, *Who Should Regulate Lawyers?*, 105 HARV. L. REV. 799, 814–19 (1992). *See generally* David B. Wilkins, *Making Context Count: Regulating Lawyers After Kaye, Scholer*, 66 S. CAL. L. REV. 1145 (1993).

10 *See* JOHN P. HEINZ & EDWARD O. LAUMANN, CHICAGO LAWYERS: THE SOCIAL STRUCTURE OF THE BAR 319–20 (1982) (finding that the legal profession consists of two categories of lawyers whose practice settings, socioeconomic and ethno-religious backgrounds, education, and clientele differ considerably); JOHN P. HEINZ ET AL., URBAN LAWYERS: THE NEW SOCIAL STRUCTURE OF THE BAR 29–47 (2005) (documenting that lawyers work in two fairly distinct hemispheres—individual and corporate—and that

efficient than hacking each of the law firms' large entity clients individually.[11] Large entity clients tend to store enormous quantities of information, though much of it may be of relatively little value to hackers, even if they had the resources to comb through it following a successful attack. For hackers, large law firms are a one-stop shop,[12] serving as filters of low value material,[13] because BigLaw will tend to receive from its clients and store only a subset of their vast information, namely, the valuable portion of it. Thus, while one might expect large law firms to be relatively well-protected, at least compared to smaller law firms, the payoff for hackers may be worth the investment.

Yet, this is not to suggest that small law firms and solo practitioners who tend to represent small businesses and individual clients[14] are not valuable depositories of client information. Rather, these lawyers may simply feature a different value proposition for hackers. For example, some of their clients may not ordinarily store sensitive information electronically and, thus, may be immune to cyberattacks. Yet, in the context of negotiating a transaction or bringing or defending a lawsuit, such clients are likely to collect information and then send it to their lawyers, who are likely to store it electronically, thus making the latter likely targets for cyberattacks.

Second, compared with their clients, lawyers are assumed to be relatively easy, vulnerable targets for cyberattacks,[15] "perceived to have fewer security resources than their clients,[16] and have less of an understanding of and appreciation for cyber risk."[17] Lawyers' relative cyber vulnerability exposes them not only to attacks seeking confidential client information, but also to hacking designed to disrupt the integrity and availability of information stored by law firms in an attempt to collect ransom payments.[18]

---

mobility between these hemispheres is relatively limited).

11 Simshaw, *supra* note 5, at 550.

12 Michael McNerney & Emilian Papadopoulos, *Hacker's Delight: Law Firm Risk and Liability in the Cyber Age*, 62 AM. U. L. REV. 1243, 1246, 1251 (2013).

13 Alan W. Ezekiel, Note, *Hackers, Spies, and Stolen Secrets: Protecting Law Firms from Data Theft*, 26 HARV. J.L. & TECH. 649, 651 (2013).

14 *See supra* note 10.

15 JANE LECLAIRE & GREGORY KEELEY, CYBERSECURITY IN OUR DIGITAL LIVES 128 (2015).

16 Simshaw, *supra* note 5, at 550–51.

17 LECLAIRE & KEELEY, *supra* note 15, at 128 (2015); RHODES & POLLEY, *supra* note 4, at 105 ("Law firms are viewed as a 'very target-rich environment' with significantly less cybersecurity protection in place than their clients have.").

18 *See, e.g.*, Joe Dysart, *'Ransomware' Software Attacks Stymie Law Firms*, A.B.A. J. (June 1, 2015, 2:30 AM), http://www.abajournal.com/magazine/article/ransomware_software_attacks_stymie_law_firms [http://perma.cc/M62F-8RT4].

Once again, attention to context is paramount to the understanding of cyberthreats; whereas lawyers representing large entity clients are likely to be less sophisticated than their clients about cyber risks and have fewer resources and expertise to deal with threats, they nonetheless represent clients who know enough to insist that their law firms take reasonable cybersecurity measures. Lawyers representing small businesses and individuals may know as little as their clients about cyberthreats, but that is no measure of comfort. Not only do such lawyers collect and store their clients' information electronically, exposing it to cyber risk, but they, too, are likely easier targets than their clients who have more to lose and, therefore, a stronger incentive to protect their sensitive information. Worse, small businesses and individuals may erroneously assume that lawyers know enough, or at least more than them about cybersecurity and that their information will be secure with their attorneys. Therefore, they insufficiently inquire and supervise their lawyers' cyber practices.

Finally, the increased competitiveness and ongoing restructuring in the legal profession, both accelerated since the Great Recession, tend to make lawyers especially vulnerable to cyberattacks. Increased competitiveness in the market for legal services has led to the emergence of a dominant "around-the-clock, 24-7" culture of availability to clients.[19] Of course, enhanced lawyer availability is often desirable from the clients' point of view, but when accomplished through mobile remote technology, it enhances cybersecurity risks.[20] Similarly, as competitive pressures lead lawyers to resort to greater use of outsourcing and artificial intelligence,[21] the benefits to clients entail an increased risk of cyberattacks.

B. Who Is Attacking the Legal Profession?

All lawyers are susceptible to attacks by malicious insiders,[22] such as disgruntled current and former lawyers and staff members, yet context matters in identifying likely hackers. Large law firms representing large entity clients involved in large-scale

---

19 Eli Wald, *Glass-Ceilings and Dead Ends: Professional Ideologies, Gender Stereotypes and the Future of Women Lawyers at Large Law Firms*, 78 FORDHAM L. REV. 2245, 2264–73 (2010).

20 McNerney & Papadopoulos, *supra* note 12, at 1251.

21 *See, e.g.*, Milton C. Regan, Jr. & Palmer T. Heenan, *Supply Chains and Porous Boundaries: The Disaggregation of Legal Services*, 78 FORDHAM L. REV. 2137 (2010); John O. McGinnis & Russell G. Pearce, *The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services*, 82 FORDHAM L. REV. 3041 (2014).

22 Simshaw, *supra* note 5, at 552.

transactional work are more likely to be targeted by social engineers, including state-sponsored hackers,[23] and subject to corporate espionage and financial crimes.[24] Smaller law firms, however, while less likely to be attacked by state-sponsored actors, still carry valuable information attractive to social engineers.[25] Government intrusion and surveillance, a growing source of cybersecurity concern for lawyers and their clients alike,[26] may be of particular concern to criminal defense, immigration, and intellectual property lawyers.[27]

C. What Lawyers Can Do About Cyberattacks

Stopping all cyberattacks is impossible to do. Yet, 96% of hacking attacks employ simple techniques, and 97% of attacks can be blocked by common security practices that are within the reach of even small law firms and solo practitioners.[28] These common practices include using current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents, avoiding the use of web-based e-mail services and public Wi-Fi, replacing the default passwords on network hardware, and training employees to recognize deceptive ("phishing") attacks.[29] Beyond these basic measures, defending effectively against cyberattacks entails making decisions about trade-offs between business needs and

---

23 *Id.*

24 McNerney & Papadopoulos, *supra* note 12, at 1264.

25 Carrie A. Goldberg, *Rebooting the Small Law Practice: A Call for Increased Cybersecurity in the Age of Hacks and Digital Attacks*, 38 AM. J. TRIAL ADVOC. 519, 521–22 (2015); *see also* Noah G. Susskind, *Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know*, 11 N.Y.U. J.L. & BUS. 573, 579 (2015) (exploring the vulnerability of smaller companies).

26 Silkenat, *supra* note 2, at 456; *see also* Sarah Jane Hughes, *Did the National Security Agency Destroy the Prospects for Confidentiality and Privilege When Lawyers Store Clients' Files in the Cloud – and What, If Anything, Can Lawyers and Law Firms Realistically Do in Response?*, 41 N. KY. L. REV. 405, 418 (2014).

27 *See, e.g.*, Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES at A1 (Mar. 29, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0 [http://perma.cc/4SPB-R96Q]; Devlin Barrett, *Justice Department Seeks to Force Apple to Extract Data from About 12 Other iPhones*, WALL ST. J. (Feb. 23, 2016), http://www.wsj.com/article_email/justice-department-seeks-to-force-apple-to-extract-data-from-about-12-other-iphones-1456202213-lMyQjAxMTI2MjIzMzMyMTMwWj.

28 VERIZON ET AL., 2012 DATA BREACH INVESTIGATIONS REPORT (2012), http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf [http://perma.cc/GTA4-3DN3].

29 Ezekiel, *supra* note 13, at 649; *see also* JOEL BRENNER, AMERICA THE VULNERABLE: INSIDE THE NEW THREAT MATRIX OF DIGITAL ESPIONAGE, CRIME, AND WARFARE 239–44 (2011).

cybersecurity.[30] For example, is a firm willing to make it more inconvenient for traveling attorneys or lawyers working remotely to access their data, in exchange for more security? When does a business imperative of providing speedy service render certain actions "worth the risk"?[31] Navigating these trade-offs and systematically assessing the cyber risks involved in doing business requires developing and putting in place a comprehensive cybersecurity plan.

The first element of a comprehensive cybersecurity plan entails involving firm leadership in learning about cybersecurity threats and making strategic decisions about them.[32] This, to be sure, does not mean that firm executives need to (or can) become cybersecurity experts. It does, however, mean that firm leaders, ranging from members of large law firms' executive committees to solo practitioners managing their own practices, must understand basic cybersecurity realities to allow them to make informed strategic judgments about: what technologies to deploy; how to mine advantages to benefit clients and the practice, and at what costs and risk level; and what security measures to employ. Because putting together a cybersecurity plan calls for strategic decision making that must involve firm management, law firms would be well-advised to task a management-level leader with specific supervisory responsibility for cybersecurity planning.

Second, lawyers must know their data—that is, be cognizant of the actual information the firm possesses and, in particular, be mindful of highly valuable and sensitive information entrusted to firm lawyers, encompassing issues such as what information firm lawyers are working with and how they are using it. Once strategic decisions are made by management, many law firms will likely delegate the implementation of cybersecurity details to non-lawyers, yet lawyer insight and exercise of judgment regarding the nature of client information and its sensitivity must inform the design of cybersecurity plans. For example, a cybersecurity plan may include different levels of protection depending on the circumstances. While a firm may prohibit all

---

30 McNerney & Papadopoulos, *supra* note 12, at 1265.

31 *Id.* at 1265–66.

32 For example, "should the firm be more worried about an attack that disrupts its networks so that attorneys lose access to information, about an attack that reveals sensitive data belonging to clients, or about an attack, that exposes the firm's own secret business data?" Or, "[w]ho are the actors that might pursue each of these attacks? What can the company do to prevent each type of attack or, if the attack happens, to manage its consequences?" *Id.* at 1265; *see also* Cheryl A. Falvey, *Demonstrating Due Diligence in Building an Information Security Program*, *in* PRIVACY AND SURVEILLANCE LEGAL ISSUES 7 (2014).

lawyers from using public cloud providers, file-sharing services for sharing documents, web-based e-mail services, and public Wi-Fi while conducting firm business, it may demand using cryptographically strong passwords only when receiving or sending highly sensitive client information. A firm may delegate the creation and maintenance of its cybersecurity plan to non-lawyers and may create guidelines for the use of various protections, but ultimately, lawyers would have to be educated to make judgment calls about what measures to use based on their knowledge of their clients' information.

Third, following a strategic, management-level risk analysis of the trade-offs between cybersecurity and business imperatives applied to the actual data a firm possesses, lawyers can then delegate day-to-day operations and implementation authority to technology experts, either within or outside the firm. A large law firm may designate someone internally within its IT department for the task, whereas a solo practitioner or a small firm may hire an outside expert to help manage its security apparatus. Day-to-day implementation of a cybersecurity plan includes two related yet distinct tasks: prevention and breach management. Prevention includes responsibility for deploying secure technologies, restricting access to high-risk activities, and implementing cybersecurity policies and procedures. For example, "blocking malware, [and] detecting anomalous behavior, such as extraction of significant quantities of data off company networks, that can indicate a cyberattack."[33] Perhaps most importantly, it entails training of lawyers and staff to observe cybersecurity practices.[34] The *Wall Street Journal* reported that "the weakest links at law firms of any size are often their own employees, including lawyers."[35] Having a plan in the event of a data breach, in turn, includes containing an ongoing cyberattack, mitigating its damage, and communicating it to clients.[36]

While lawyers in general may delegate to cybersecurity experts the implementation of cybersecurity plans, complex legal ethics questions may arise requiring the insight, approval, and supervision of lawyers. For example, consider the use of honeypots, cybersecurity mechanisms set to detect, deflect, and counteract attempts at unauthorized access to protected

---

33 McNerney & Papadopoulos, *supra* note 12, at 1268.

34 Simshaw, *supra* note 5, at 568–69.

35 Jennifer Smith, *Lawyers Get Vigilant on Cybersecurity*, WALL ST. J. (June 26, 2012, 4:09 PM), http://www.wsj.com/articles/SB10001424052702304458604577486761101726748.

36 *See* Mercedes Kelley Tunstall, *The Path to Comprehensive Cybersecurity Laws in the United States*, *in* UNDERSTANDING DEVELOPMENTS IN CYBERSPACE LAW 61, 63 (2015 ed. 2015).

information. Generally, honeypots consist of data that appears to be legitimate and thus of value to attackers, but is in fact deceptive information planted to attract hackers who are then tracked and blocked.[37] Among cyber experts, while risky, honeypots are considered a valid information security tactic.[38] Yet, whether law firms can deploy honeypots raises a complicated and unresolved question under the Rules, which generally prohibit lawyers from engaging in dishonest or deceptive practices in the practice of law.[39] Notably, it is a question lawyers need to be made aware of and help resolve.

Finally, law firms must develop a strong culture of cybersecurity,[40] because cyber "compliance and risk management intertwine around corporate culture."[41] Lawyers and staff who think of cybersecurity as somebody else's problem or responsibility are prone to make the very mistakes, like opening phishing e-mails, that expose a firm to heightened risk. Since a law firm's cybersecurity apparatus is only as safe as its weakest link, lawyers and staff must be trained to conceive of cybersecurity not as an imposition on doing business, but as an integral part of firm culture—that is, to move past thinking of business considerations and cybersecurity as a trade-off and accept cybersecurity as a business need.[42]

Context is likely to play an important role in the implementation of cybersecurity plans. Some security measures, indeed, even some basic security measures such as avoiding the use of web-based e-mail services and public Wi-Fi, as well as expensive training, may be out of reach for some solo practitioners and smaller law firms. Yet, as Carrie Goldberg points out, it is in these very types of attorney-client relationships that an attorney is likely to be "more stringent and informed than the client about necessary information security measures."[43] In such instances, a lawyer can enhance the cybersecurity of the attorney-client relationship by explaining to the client the lawyer's limited means and the risks entailed, and communicating the shared responsibility to maintain privacy,

---

37 *See* Sean L. Harrington, *Cyber Security Active Defense: Playing with Fire or Sound Risk Management?* 20 RICH. J.L. & TECH. 12, 14–16 (2014).

38 *Id.* at 15.

39 MODEL RULES OF PROF'L CONDUCT r. 8.4(c) (AM. BAR ASS'N 2013); *see, e.g.*, *In re* Pautler, 47 P.3d 1175 (Colo. 2002) (disciplining an assistant district attorney who misrepresented himself to a suspected murderer as a public defender); *see also In re Gatti*, 8 P.3d 966 (Or. 2000) (disciplining a lawyer who misrepresented himself as a medical professional in order to obtain information related to the representation of a client).

40 McNerney & Papadopoulos, *supra* note 12, at 1266.

41 Susskind, *supra* note 25, at 608.

42 *Id.* at 608–12.

43 Goldberg, *supra* note 25, at 543.

especially as it pertains to a client's voluntary online behavior and habits.[44]

II. THE UNDERREGULATION OF LAWYERS' CYBERSECURITY CONDUCT

Critics from the left and the right have long disparaged professional ideologies, and rules of professional conduct that implement and codify them, as self-serving rhetorical tools meant to justify the profession's power and status,[45] monopoly over the provision of legal services, and anticompetitive fees.[46] At first glance, the recent flurry of changes to Rules regarding cybersecurity[47] appear unnecessary, and thus susceptible to this criticism. To begin with, the Rules have long required lawyers to protect confidential information and so the promulgation of subsection 1.6(c), stating in relevant part that "a lawyer shall make reasonable efforts to prevent the . . . unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,"[48] seems like a redundant clause, a rhetorical nod regarding cybersecurity. Similarly, the Rules have long demanded competence and so the revision of Comment 8 to Rule 1.1, stating in relevant part that "to maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology* . . . ,"[49] seems perfunctory. Moreover, the changes appear unnecessary because on initial consideration one would expect clients' reactions, such as firing a law firm following a security breach, withholding new business, or filing a malpractice lawsuit, to provide lawyers with ample motivation and incentive to reasonably protect clients' information. Cybersecurity thus appears to be the posterchild for advocates of market controls and deregulation; instead of promulgating new rules of professional conduct, let the market regulate lawyers' cybersecurity conduct.

Closer scrutiny, however, reveals that liability rules (e.g., malpractice suits) and market controls (e.g., termination of the attorney-client relationship) are not likely to effectively regulate lawyers' cybersecurity conduct.[50] Generally, a plaintiff in a

---

44 *Id.*

45 *See, e.g.*, RICHARD L. ABEL, AMERICAN LAWYERS (1989); MAGALI S. LARSON, THE RISE OF PROFESSIONALISM: A SOCIOLOGICAL ANALYSIS (1977).

46 RICHARD A. POSNER, THE PROBLEMATICS OF MORAL AND LEGAL THEORY 185–211 (1999).

47 *See infra* Section III.A.

48 MODEL RULES OF PROF'L CONDUCT r. 1.6(c) (AM. BAR ASS'N 2013).

49 *Id.* r. 1.1 cmt. 8 (emphasis added).

50 For a review of disciplinary, liability, institutional, legislative, and market

malpractice lawsuit must establish four elements: the existence of a duty, breach of the duty owed, causation, and damages.[51] Yet a plaintiff in a malpractice suit alleging negligence in failing to protect information is unlikely to be able to prove "damages because of the challenges in answering key questions about cybersecurity breaches: who perpetrated the cyberattack; 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 reputational damage, resulted for the victim?"[52] Consequently, there are hardly any cases litigating attorney (or even corporate) negligence for failure to protect confidential information.[53]

The same challenges—not knowing who perpetrated the cyberattack; what information they stole; what is the value of that information to them or others; and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim—limit the ability of clients to fire or otherwise sanction a law firm for failing to protect confidential information. Worse, clients are often prevented from reacting to lawyers' cybersecurity inaction because they do not find out about it. To be sure, some clients, usually sophisticated and powerful entity clients, have been pressuring their law firms to put in place cybersecurity measures and others have demanded being advised of security breaches.[54] Yet lawyers are under no general duty to report attacks to clients,[55] often do not learn about attacks themselves,[56] and when lawyers do find out about attacks, they often have insufficient information to allow for comprehensive reporting to clients.

Thus, clients often do not find out about lawyers' cybersecurity breaches, and when they do, they have insufficient information on which to respond or to successfully sue. Unfortunately, underregulation—the inability of clients to effectively utilize liability rules and market controls to ensure that lawyers face appropriate cyber incentives—compounds the

---

controls, see Wilkins, *Who Should Regulate Lawyers?*, *supra* note 9, at 804–19. *See generally* David B. Wilkins, *How Should We Determine Who Should Regulate Lawyers? Managing Conflict and Context in Professional Regulation*, 65 FORDHAM L. REV. 465 (1996).

51 RONALD E. MALLEN & ALLISON MARTIN RHODES, LEGAL MALPRACTICE: THE LAW OFFICE GUIDE TO PURCHASING LEGAL MALPRACTICE INSURANCE § 1:2 (2016).

52 McNerney & Papadopoulos, *supra* note 12, at 1261.

53 *Id.* at 1260; *see also* Hughes, *supra* note 26, at 426 ("[M]ost data breach class actions have been dismissed for lack of damages.").

54 *See, e.g.*, Monica Bay, *Understanding the Risks to Cybersecurity: Large Law Firms Are Viewed as Vulnerable and Store Information that Hackers Know Is Valuable*, 36 NAT'L L.J. 28, 28 (2014).

55 *See infra* Section III.A.

56 Simshaw, *supra* note 5, at 550–51.

underlying problem. As lawyers face insufficient incentives to implement appropriate cybersecurity measures and report attacks to clients, data about attacks and their consequences goes uncollected, diminishing the prospects of effective liability rules and market controls developing in the future. This is the kind of market failure that is unlikely to resolve itself without regulatory intervention, except that liability rules are not likely to constitute an effective regulatory response. It is also the kind of market failure that prevents the collection of the very data we need to better understand the extent of the problem we are facing.

To be sure, underregulation does not mean that lawyers face no regulatory forces pertaining to their cybersecurity conduct. To begin with, legislative controls regulate the cyber conduct of lawyers. State laws impose on lawyers, and others who hold personal information about customers, data breach notification duties if they reasonably believe that an unauthorized party has obtained the customers' information.[57] In addition, various federal statutes address data breach in specific industries. For example, attorneys working in the health care industry who have access to covered information are subject to the privacy and security provisions of the Health Insurance Portability & Accountability Act;[58] other federal statutes generally regulating data security may apply to lawyers as well.[59]

Next, even in the absence of reported malpractice decisions regarding failure to protect confidential client information, liability rules may indirectly inform attorneys' cyber conduct. For example, law firms accused of cybersecurity misconduct by clients may decide to settle cases to avoid having to publicly defend suits risking exposure of embarrassing cyber details and consequential reputational harm. Similarly, market controls may also inform lawyers' conduct, even if clients do not learn about cyberattacks and compromised information. Powerful clients can demand that their lawyers establish reasonable cybersecurity policies, and some lawyers, even in the absence of a duty to disclose information to clients about cyberattacks, may reveal information to build trust in the attorney-client relationship or to avoid undermining it upon subsequent disclosure. Other lawyers may take cybersecurity action to comply with insurance companies' protocols, even if the risk of malpractice liability is remote.

---

57 McNerney & Papadopoulos, *supra* note 12, at 1254–55.

58 Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

59 McNerney & Papadopoulos, *supra* note 12, at 1256 (describing guidelines advising corporations and attorneys to report material cyber risks and incidents to the SEC).

Yet other lawyers may respond to social norms, such as peer pressure and organically evolving norms within their legal communities. For example, as cybersecurity awareness increases, and Continuing Legal Education providers flood the marketplace with offerings, lawyers may be induced to take a class to keep up with the competition. Also, as younger attorneys, likely more tech-savvy, join the profession, law firms become both more aware of cyber conduct and more apt to engage with it more directly.

In sum, while the ineffectiveness of traditional liability rules and market controls results in the systematic underregulation of lawyers' cybersecurity conduct, other regulatory controls have led to significant changes in the cyber habits of some members of the legal profession, such as the increased use of two-factor authentication in lieu of a single password to access secure systems.[60] Before turning to explore rules of professional conduct as a possible remedy to lawyers' likely cybersecurity inaction, a word about Holmesian bad people.[61] Since we do not know enough about the extent and scope of cyberattacks against lawyers, admittedly in part because lawyers do not gather or share this information, why assume that lawyers do not do enough to protect their clients' information and best interests? Even conceding a legal world of increased atomism and individualism, one in which lawyers and their clients seek to maximize their short-term interests with little regard to the impact on others,[62] why assume that, but for regulatory intervention, most or even many lawyers will act as Holmesian bad people and try to get away with implementing insufficient cybersecurity measures? Surely some lawyers will do the right thing by their clients simply because it is the right thing to do.

Regrettably, in addition to the dominance of individualism (or the hired gun ideology)[63] and the relative decline of relational approaches in legal (and business) decision making made by both clients and lawyers,[64] three interrelated reasons suggest that,

---

60 *See, e.g.*, Ellen Blanchard & Rodney Blake, *Law Firms Are the New Target for IP Theft: Basic Protections*, IPWATCHDOG (June 19, 2015), http://www.ipwatchdog.com/2015/06/19/law-firms-are-the-new-target-for-ip-theft-basic-protections/id=58656/ [http://perma.cc/3G3U-9UBY].

61 *See* Russell G. Pearce & Eli Wald, *Rethinking Lawyer Regulation: How a Relational Approach Would Improve Professional Rules and Roles*, 2012 MICH. ST. L. REV. 513, 522–23 (2012).

62 *See* Russell G. Pearce & Eli Wald, *The Obligation of Lawyers to Heal Civic Culture: Confronting the Ordeal of Incivility in the Practice of Law*, 34 U. ARK. LITTLE ROCK L. REV. 1, 26–39 (2011).

63 *See generally* William H. Simon, *The Ideology of Advocacy: Procedural Justice and Professional Ethics*, 1978 WIS. L. REV. 29 (1978).

64 Pearce & Wald, *supra* note 62; Russell G. Pearce & Eli Wald, *The Relational Infrastructure of Law Firm Culture and Regulation: The Exaggerated Death of Big Law*,

absent regulatory intervention, some lawyers are likely to try to get away with offering insufficient cyber protection to clients and acting as Holmesian bad people.

First, implementing effective cybersecurity measures can entail significant expenses. While some costs can be easily rolled onto clients, for example, expenses directly related to undertaking specific measures in connection with the representation of clients with known security risks and needs, other expenses, such as the cost of upgrading the entire cybersecurity apparatus of the firm or the time investment of lawyers and staff learning about the apparatus, may be harder to recoup.

Second, even when the costs of implementing cybersecurity measures can be recouped, lawyers are notoriously technophobic.[65] To be sure, some lawyers are at the forefront of using new technological advances to better serve clients.[66] Yet the legal profession has a long, documented history of resisting technological advances due to ignorance,[67] vanity,[68] status envy,[69] and independence,[70] which suggests that, left to their own devices, lawyers are unlikely to implement the necessary cybersecurity measures to protect clients' information.

Finally, some cybersecurity measures, such as limiting access to unsecure networks and mobile devices, abstaining from using portable drives, frequent change of passwords, and timely lock down of computers in and out of the office, are likely to be perceived to be, and indeed are, cumbersome for lawyers. This is especially true for older and less technology-savvy attorneys, some of whom, by virtue of their seniority, are also likely to be powerful within their firms and therefore harder to reign in. In sum, because liability rules and market controls are unlikely to provide lawyers with a sufficient incentive to take appropriate cybersecurity action, and because implementing effective cybersecurity measures is expensive, time-consuming, and inconvenient, some lawyers are unlikely to reasonably protect their clients' information absent regulatory intervention.

---

42 HOFSTRA L. REV. 109, 110 (2013).

65 Timothy J. Toohey, *Beyond Technophobia: Lawyers' Ethical and Legal Obligations to Monitor Evolving Technology and Security Risks*, 21 RICH. J.L. & TECH. 9 (2015).

66 *See* William Henderson, *What the Jobs Are: New Tech and Client Needs Create a New Field of Legal Operations*, A.B.A. J. (Oct. 1, 2015, 6:00 AM), http://www.abajournal.com/magazine/article/what_the_jobs_are [http://perma.cc/WHB9-E4UC].

67 *See, e.g.*, Brian E. Finch, *The Legal Profession Needs to Get Smart About Cybersecurity*, NAT'L L.J. 27, at 27 (2015).

68 Vivia Chen, *Why is 'Phooling' a Lawyer So Easy?*, NAT'L L.J. 5, at 5 (2015).

69 Ezekiel, *supra* note 13, at 656.

70 *Id.*

III. THE LEGAL ETHICS OF CYBERSECURITY

Professional ideologies and rules of professional conduct promulgated by lawyers are often self-serving and warrant a healthy dose of skepticism, yet at the same time, they play an important and effective role in the regulation of lawyers. As liability rules, the rules of professional conduct—part and parcel of state law—define misconduct and give rise to a disciplinary system that incentivizes lawyers to comply with them.[71] As the embodiment of professionalism, rules of professional conduct are social norms that shape and guide the conduct of lawyers. Thus, notwithstanding criticisms of rules of professional conduct and acknowledging their chronic underenforcement,[72] legal ethics rules can play an important role in the regulation of lawyers.[73]

A. The Current Legal Ethics Stance on Cybersecurity

To their credit, the Rules have been revised in recent years to take account of technological changes impacting the practice of law. In August 2012, the ABA House of Delegates renumbered Comment 6 to Rule 1.1 on competence as Comment 8 and added a clause calling on lawyers to keep abreast of relevant technology affecting their practice. While the revision was made to a Comment rather than in the body of the Rule, was aspirational rather than mandatory, and failed to explicitly identify cybersecurity as a concern or a priority (stating instead that "to maintain the requisite knowledge and skill" mandated by Rule 1.1, "a lawyer *should* keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . ."),[74] the Comment revision was not without practical impact. It does open the door to discipline, designating ignorance of relevant technology as incompetence and thus misconduct, and, by identifying knowledge of relevant technology as a component of competence, it did help give rise to a cottage industry of Continuing Legal Education courses about cybersecurity.[75] Notably, however, the Comment does not deem

---

71 MODEL RULES OF PROF'L CONDUCT r. 8.4(a) (AM. BAR ASS'N 2013). Rules of professional conduct also establish standards of conduct which inform determination of civil liability for malpractice. *See id.* at Preamble & Scope ¶ 20.

72 Richard L. Abel, *Why Does the ABA Promulgate Ethical Rules?*, 59 TEX. L. REV. 639, 648 (1981) ("[S]tudy after study has shown that the current rules of professional conduct are not enforced."); Wilkins, *Legal Realism for Lawyers*, *supra* note 9, at 493 (noting that the rules of professional conduct tend to be "systematically underenforced").

73 Richard H. McAdams, *The Origin, Development, and Regulation of Norms*, 96 MICH. L. REV. 338 (1997) (discussing how legal norms and rules affect professional conduct).

74 MODEL RULES OF PROF'L CONDUCT r. 1.1 cmt. 8 (emphasis added).

75 Darla W. Jackson, *Cybersecurity: Breaches and Heartbleed to BYOD – Are Bankers, Entertainment Company Executives, Celebrities, Postal Workers, Ice Cream Lovers, Home*

the failure to utilize technology or inaction with regard to technological risks as incompetent conduct. Rather, all it recommends is keeping abreast of benefits and risks of relevant technology.

Arguably, a more significant change was made to Rule 1.6 on confidentiality. Elevating a Comment to a new subsection of Rule, 1.6(c), the Rule now mandates that "[a] lawyer shall make *reasonable efforts* to prevent . . . the unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[76] Importantly, exactly because the dearth of malpractice litigation regarding failure to protect information results in lack of judicial exposition of reasonableness, new Comments 18 and 19 to Rule 1.6 do offer a partial definition of reasonable efforts.

After emphasizing the central role of reasonableness, stating that "[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure,"[77] Comment 18 adds that:

> [f]actors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[78]

Comment 19 similarly identifies reasonableness as a key term of art, adding that "[w]hen transmitting a communication that includes information relating to the representation of a client,"[79] that is, confidential information,[80]

> 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.[81]

Builders, and CIOs the Only Ones Who Should Be Concerned?, 106 L. LIBR. J. 633, 638 (2014) (noting that the A.B.A. has begun offering a Cybersecurity Series); *see also ABA Cybersecurity Series*, A.B.A., http://www.americanbar.org/content/ebus/events/ce/cyber-security-core-curriculum.html [http://perma.cc/6X3H-LN49].

76 MODEL RULES OF PROF'L CONDUCT r. 1.6(c) (emphasis added).

77 *Id.* r. 1.6 cmt. 18.

78 *Id.*

79 *Id.* r. 1.6 cmt. 19.

80 *Id.* r. 1.6(a).

81 *Id.* r. 1.6 cmt. 19 (emphasis added).

Comments 18 and 19 take a first important step in defining the meaning of "reasonable efforts" to protect clients' information. They correctly identify reasonableness as a key element in assessing cybersecurity measures, and they begin to define the term, referring to the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients as relevant considerations of reasonableness.

Yet Rule 1.6(c) and Comments 18 and 19 fall short in several respects. First, they fail to require that lawyers put in place a cybersecurity plan which will regularly monitor their cybertechnology to detect breaches. Perhaps the Comment implies a duty to regularly monitor one's cybersecurity measures, after all, how can a lawyer assess "the likelihood of disclosure if additional safeguards are not employed" without monitoring the performance of existing safeguards? Similarly, assessing "the cost of employing additional safeguards" as well as "the difficulty of implementing the safeguards" implies a duty to assess one's existing apparatus. But the Comments fail to explicitly identify a duty to implement a cybersecurity plan, a noteworthy omission given that elsewhere the Comments do explicitly impose similar duties. For example, while a duty to monitor for conflicts of interest may be implied from a Rule prohibiting conflicts of interest, Comment 3 to Rule 1.7 on conflicts of interest explicitly states that:

> [t]o determine whether a conflict of interest exists, a lawyer should adopt reasonable procedures, appropriate for the size and type of firm and practice, to determine . . . the persons and issues involved . . . . Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule.[82]

Yet, while ignorance about cybersecurity attacks and their scope appears to be the norm, the Comment to Rule 1.6 fails to explicitly demand monitoring for cyberattacks akin to the monitoring of conflicts of interest.

Second, Rule 1.6(c) and its Comment do not sufficiently clarify what constitutes "reasonable efforts" and "reasonable precautions." Perhaps, in a world of constantly evolving technology, the Comment avoided specifying the nature of appropriate measures to prevent it from quickly becoming antiquated. Curiously, however, the Comment did not shy away

---

82 *Id.* r. 1.7 cmt. 3.

from delving into the meaning of reasonableness when such analysis benefited lawyers. Comment 19 states in relevant part that "[t]his duty," to take reasonable precautions to prevent the unauthorized disclosure of client information, "however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[83] This innocent sounding clause implicitly refers to ABA Formal Opinion 99-413, in which the ABA Standing Committee held that "[a] lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the [Rules] because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[84]

In other words, Comment 19, while ostensibly staying clear of defining the meaning of "reasonable efforts," nonetheless states that the use of unencrypted e-mail by lawyers is reasonable because apparently unencrypted e-mails "afford[] a reasonable expectation of privacy" based on Formal Opinion 99-413, which found that "[t]he same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail."[85] The point, to be clear, is not to debate whether the Committee's conclusion, made in 1999, that unencrypted e-mails afford a reasonable expectation of privacy, still holds true presently, although some have characterized the conclusion as "misguided."[86] Rather, it is that what Comment 19 does half-heartedly and indirectly[87]—delving into the definition of reasonable efforts—it ought to do openly and clearly.

Third, Rule 1.6(c) and its Comment fails to mandate disclosure to clients regarding cyberattacks and/or security breaches regarding client information. There are at least two possible good faith explanations for this omission. To begin with, attorney-client communications are generally governed by Rule 1.4, not Rule 1.6, and so there would be no reason to require communications regarding cybersecurity in the latter. Yet the

---

83 *Id.* r. 1.6 cmt. 19.

84 A.B.A. Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) (discussing protection of confidentiality by means of unencrypted e-mail).

85 *Id.*

86 Toohey, *supra* note 65, at 23; *see also* Rebecca Bolin, *Risky Mail: Concerns in Confidential Attorney-Client Email*, 81 U. CIN. L. REV. 601, 618–21 (2012) (discussing and critiquing the effect of 99-413).

87 Curiously, Comment 19 fails to identify Formal Opinion 99-413, although it appears to cite its language. *Compare* MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 19 (AM. BAR ASS'N 2013), *with* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

Rules and Comments often explicitly cross-reference other Rules such that the failure to reference Rule 1.4 is glaring. Indeed, Comment 18 does reference Rules 1.1, 5.1, and 5.3, making the omission to reference Rule 1.4 inexplicable. Next, Comments 18 and 19 do implicitly reference Rule 1.4, both stating in relevant part that "[a] client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule."[88] Rule 1.4(a)(1), in turn, states in relevant part that "[a] lawyer shall promptly inform the client of any decision or circumstance with respect to which the client's informed consent . . . is required,"[89] such that one could argue that the Comments 18 and 19 indirectly reference Rule 1.4 (by referring to informed consent, which requires communicating with clients). But even viewed in the light most favorable to the Rules, such indirect reference to Rule 1.4 is lacking as it fails to require disclosure to clients of cybersecurity attacks or breaches. It only indirectly triggers a duty to communicate regarding forgoing security measures as opposed to imposing a general duty to communicate regarding cybersecurity. Furthermore, Comments 18 and 19 fail to reference the subsections of Rule 1.4 that may give rise to a duty to communicate regarding cybersecurity concerns, namely 1.4(a)(2), 1.4(a)(3), and 1.4(b).

Notwithstanding the silence of Rule 1.6(c), does Rule 1.4 independently require lawyers to communicate with clients regarding cybersecurity, let alone advise clients about cyberattacks against the law firm and/or breaches of security? Most commentators opining on this issue believe the Rules do not impose such a duty,[90] and regrettably they appear to be right because the Rules essentially only mandate disclosure of material information to clients, and the usual uncertainty engulfing cyberattacks casts an inherent doubt on the materiality of cyberattacks and resulting breaches.

Rule 1.4(a)(2) states that "[a] lawyer shall . . . reasonably consult with the client about the means by which the client's objectives are to be accomplished."[91] Cybersecurity measures certainly qualify as part of the *means* by which the client's objectives are to be accomplished, and thus would support an interpretation pursuant to which a lawyer must reasonably

---

88 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 18.

89 *Id.* r. 1.4(a)(1).

90 *See, e.g.*, Ezekiel, *supra* note 13, at 653 ("Most astonishingly, the existing professional responsibility standards generally *do not require any disclosure to the client* when client information is stolen from a law firm.").

91 MODEL RULES OF PROF'L CONDUCT r. 1.4(a)(2).

consult with the client about reasonable security measures, for example, whether to encrypt communications regarding the representation, but the Rule falls short of explicitly demanding such a communication. Therefore, if a lawyer has in place cybersecurity measures, or reasonably believes that his cybersecurity measures or lack thereof are sufficient, Rule 1.4(a)(2) does not appear to require any communication whatsoever. Worse, Rule 1.4(a)(2) says nothing whatsoever about cyberattacks or security breaches.

Rule 1.4(a)(3) states that "[a] lawyer shall keep the client reasonably informed about the status of the matter,"[92] and Comment 3 adds that "paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation."[93] If cybersecurity measures are to be construed as the "*means* by which the client's objectives are to be accomplished," they are certainly not the *matter*, and thus, 1.4(a)(3) appears not to generally apply to cybersecurity communications. However, a significant cybersecurity breach that results in the disclosure of otherwise confidential and privileged information, or that foils the negotiation of a transaction on behalf of a client, can certainly impact the status of a matter. Comment 3 supports that interpretation because a significant cybersecurity breach would be a "significant development" affecting the substance of the representation.[94]

In any event, however, Rule 1.4(a)(3) falls short of imposing a general duty of communication regarding cybersecurity attacks and breaches. Rather, it only mandates disclosure to clients of significant cyber breaches which constitute a significant development and result in an impact regarding the status of the representation. Moreover, the same considerations that obscure clients' ability to prove damages resulting from a lawyer's failure to reasonably protect information—not knowing who perpetrated the cyberattack, what information they stole, what the value of that information is to them or others, and what other harms, such as operational disruption, competition, or reputational damage, resulted for the victim—would often shield lawyers from discipline for violating 1.4(a)(3). If a lawyer does not know who perpetrated the cyberattack, what information was stolen, what the value of that information is to them or others, and what other

---

92 *Id.* r. 1.4(a)(3).

93 *Id.* r. 1.4 cmt. 3.

94 *See* Colo. Bar Ass'n Ethics Comm., Formal Ethics Op. 113 (Nov. 19, 2005) (discussing the ethical duties of an attorney to disclose errors to a client).

harms resulted for the client, how could a lawyer ever conclude that a breach constitutes a "significant development"?

Rule 1.4(b) states that "[a] lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation."[95] While Rule 1.4(b) appears to only apply to explaining the "matter" at hand, Comment 5 importantly clarifies that:

> [t]he client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation *and the means by which they are to be pursued* . . . . The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation.[96]

Rule 1.4(b) arguably gives rise to a general duty to communicate regarding cybersecurity and, in particular, about cyberattacks and breaches because cybersecurity measures are part of the means by which the client's objectives are to be pursued. Thus, the client should receive sufficient information from the lawyer to be able to participate intelligently in decisions concerning cybersecurity. ABA Formal Opinion 95-398 lends support to this interpretation, finding that "should a significant breach of confidentiality occur . . . a lawyer may be obligated to disclose such breach to the client or clients whose information has been revealed,"[97] citing Rule 1.4(b), and adding that "[w]here the unauthorized release of confidential information could reasonably be viewed as a significant factor in the representation, for example where it is likely to affect the position of the client or the outcome of the client's legal matter, disclosure of the breach would be required under Rule 1.4(b)."[98] Yet, like Rule 1.4(a)(3), the communication appears to be mandated only with regard to severe cyberattacks with significant impact on a client, or limited to communications regarding cybersecurity "means" rather than a clear general duty requiring communication regarding cybersecurity measures, attacks, and breaches.[99]

Some commentators have argued that Rule 1.15 on safekeeping property pertains to protecting client information because Rule 1.15(a) states, *inter alia*, that "other property," presumably including information, "shall be . . . appropriately safeguarded."[100] No doubt Rule 1.15 applies, if only to impose on lawyers a duty to monitor client trust accounts for cyberattacks

---

95 MODEL RULES OF PROF'L CONDUCT r. 1.4(b).

96 *Id.* r. 1.4 cmt. 5 (emphasis added).

and breaches.[101] Yet, the application adds little to Rules 1.6(a) and 1.6(c), which impose a general duty to protect clients' confidential information from unauthorized disclosure.

Rule 5.1, regarding responsibilities of supervisory lawyers to other lawyers, and Rule 5.3, regarding supervisory responsibilities to non-lawyer assistance, have been slightly revised to reflect technological changes. Read together, Rules 5.1 and 5.3 require some lawyers to supervise the conduct of other lawyers and non-lawyers inside and outside of the practice. They state that supervisory lawyers "shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that,"[102] first, "all lawyers in the firm conform to the Rules of Professional Conduct,"[103] including Rules, such as 1.1 and 1.6 pertaining to cybersecurity, and second, that the conduct of non-lawyers employed by, retained by, or associated with the lawyer, "is compatible with the professional obligations of the lawyer."[104] As one commentator notes:

> These rules reflect the notion that a law firm's data security practices are only as strong as its weakest link. As a result, lawyers must make sure that subordinate attorneys, interns, paralegals, case managers, administrative assistants, and external business partners all understand necessary data security practices and the critical role that all parties play in ensuring the protection of client information.[105]

In addition, these changes make modest positive contributions to lawyers' understanding of new technological realities. For example, the title of Rule 5.3 was changed from

---

97 ABA Comm. on Ethics & Prof'l Resp., Formal Op. 95-398 (1995).

98 *Id.*; *see also* N.H. Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013), https://www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp ("Where highly sensitive data is involved, it may become necessary to inform the client of the lawyer's use of cloud computing and to obtain the client's informed consent."); Pa. Bar Assoc., Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2011-200 (2011), http://www.slaw.ca/wp-content/uploads/2011/11/2011-200-Cloud-Computing.pdf [http://perma.cc/GJ87-T8TS] ("While it is not necessary to communicate every minute detail of a client's representation, 'adequate information' should be provided to the client so that the client understands the nature of the representation and 'material risks' inherent in an attorney's methods.").

99 See also Alaska Rule 5.3(d) (2014), dictating that "[a] lawyer who learns that any person employed by the lawyer has revealed a confidence . . . protected by these rules shall notify the person whose confidence or secret was revealed." Importantly, however, the rule does not generally apply to a law firm experiencing a cyberattack and compromised information but rather only to a third party employed by the law firm.

100 MODEL RULES OF PROF'L CONDUCT r. 1.15(a); *see also* Goldberg, *supra* note 25, at 529–30; Hughes, *supra* note 26, at 415–16.

101 Christine Daleiden, *Information Security Basics for Lawyers*, 18 HAW. B.J. 4, 8–9 (2014).

102 MODEL RULES OF PROF'L CONDUCT r. 5.1.

103 *Id.*

104 *Id.* r. 5.3.

105 Simshaw, *supra* note 5, at 563.

"Responsibilities Regarding Nonlawyer *Assistants*," to "Responsibilities Regarding Nonlawyer *Assistance*," to capture the notion that technology, including cybertechnology, assists lawyers in the practice of law. Rule 5.3, providing examples of the use of non-lawyers outside the firm, offers "using an Internet-based service to store client information" as an illustration.[106]

Yet, Rules 5.1 and 5.3, once again, forgo an opportunity to take a clear detailed stance regarding cybersecurity efforts and measures. For example, Comment 2 on Rule 5.1 states that "[p]aragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Rules,"[107] and goes on to give examples of such "internal policies and procedures," a perfect opportunity to require cybersecurity measures, including the adoption of cybersecurity plans. Instead, it states "[s]uch policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised."[108]

Similarly, while Comment 3 on Rule 5.3 identifies lawyers' use of cloud computing as a form of non-lawyer assistance, it fails to detail any of the efforts and measures lawyers must employ in conjunction with the use of this technology. Instead, it generically states that: "[w]hen using such services outside the firm, a lawyer *must make reasonable efforts* to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations," adding that "[t]he extent of this obligation will depend upon the circumstances, including the education, experience and reputation of the nonlawyer; the nature of the services involved; [and] the terms of any arrangements concerning the protection of client information."[109] In other words, the Rules once again invoke reasonableness without specifying its content and a commitment to protecting confidentiality without specific guidance as to the cybersecurity measures lawyers must put in place.

Lawyers' use of cloud computing has been the subject of various ethics opinions that serve as a revealing example of how

---

106 MODEL RULES OF PROF'L CONDUCT r. 5.3 cmt. 3.

107 *Id.* r. 5.1 cmt. 2.

108 *Id.* Arguably, given Rule 1.15's requirement that lawyers protect clients' property, including clients' trust accounts, Comment 2 could be read to demand cybersecurity measures to protect such accounts, but this would be at best an implied requirement.

109 *Id.* r. 5.3 cmt. 3.

ethics committees follow the lead of the Rules and offer only a limited insight into the meaning of reasonableness. Ethics opinions generally hold that cloud computing is permissible, as long as lawyers take reasonable steps when selecting and using services.[110] Notably, some states appear to impose additional, specific cybersecurity measures (Iowa requires lawyers to "[d]etermine the degree of protection the vendor provides to its clients' data"; New Jersey requires lawyers to "[m]ake sure that vendors are using available technology to guard against foreseeable infiltration attempts"; and North Carolina demands that its lawyers "[e]valuate the vendor's security and backup strategy"), and *The ABA Cybersecurity Handbook* wisely acknowledges that "[l]awyers should monitor and reassess the protections of the cloud provider as the technology evolves."[111] How lawyers are to go about meeting these requirements, however, is less than clear. As Drew Simshaw points out, "[i]t is also worth noting the limits of a lawyer's duties under the rules,"[112] according to these ethics opinions. For example, in New Hampshire, "a lawyer's duty is to take reasonable steps to protect confidential client information, not to become an expert in information technology," and "[w]hen it comes to the use of cloud computing, the Rules of Professional Conduct do not impose a strict liability standard."[113]

All in all, the ABA must be commended for its proactive approach to addressing the evolving impact of technology on law practice. New subsection 1.6(c) explicitly identifies protection of client information, including cybersecurity measures, as a priority, and moving the language from a Comment to the body of the Rules signifies to lawyers the emphasis the Rules now place on information protection.[114] Next, the new subsection takes a first important step in shifting lawyers' focus from avoiding

---

110 *Cloud Ethics Opinions Around the U.S.*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloudethics-chart.html [http://perma.cc/VY84-VA7P]. In addition, *The ABA Cybersecurity Handbook* contains an appendix of "Ethics Opinions on Lawyer Confidentiality Obligations Concerning Cloud Computing." RHODES & POLLEY, *supra* note 4, at 245.

111 *Id.* at 77.

112 Simshaw, *supra* note 5, at 565.

113 N.H. Bar Ass'n Ethics Comm., Advisory Op. #2012-13/4 (2013), *supra* note 98.

114 For an excellent analysis of the Rules' new approach to cybersecurity, see generally Judith L. Maute, *Facing 21st Century Realities*, 32 MISS. C. L. REV. 345 (2013). The ABA has tried to stay at the forefront of enhancing lawyers' cybersecurity awareness. For example, in April 2016, ABA President Paulette Brown offered ABA members an opportunity to receive FBI cybersecurity alerts, noting that, "the ABA is keenly aware of the increase in efforts to hack into the computer systems of legal professionals to reach the significant amounts of non-public information they hold." *See* E-mail from Paulette Brown, President, Am. Bar Ass'n, to ABA Members (Apr. 12, 2016, 2:00 AM) (on file with author).

negligent and inadvertent disclosure to the new landscape of affirmatively protecting client information from unauthorized access by third parties. Moreover, Comments 18 and 19 to Rule 1.6 help clarify the meaning of the duty to protect client information by specifying the factors that render protective measures reasonable. Appropriate references to this new approach are made in Rules 1.1, 1.15, 5.1, and 5.3. Yet the Rules do not do enough to guide lawyers' cybersecurity conduct, especially given that liability rules and market controls are not likely to incentivize lawyers to sufficiently protect client information.

B. Responding to the New Frontier: The Future of Legal Ethics in the Age of Hackers and Cyberthreats to Clients' Information

The Rules embody, and have long taken, a one-size-fits-all, universal approach to the regulation of lawyers' conduct.[115] As such, they cannot, and should not, be amended frequently to reflect minor changes in the practice of law. Rather, the Rules are open-ended standards that can and should accommodate practice changes, for example via clarifying formal ethics opinions. However, sometimes changing practice realities do necessitate revisions to the Rules, and in such circumstances the Rules must be revised so they can continue to inform and guide lawyers' actual practice and avoid becoming antiquated.[116]

Cybersecurity is one such instance that necessitates changing the Rules. Protecting confidential client information, a fundamental tenet of law practice, used to be about avoiding negligent inadvertent disclosure. Typical examples of misconduct were leaving one's notes or laptop unattended in a conference room, or inadvertently disclosing confidential information to opposing counsel over e-mail.[117] Hackers, however, present a different challenge, one of affirmatively protecting information from unauthorized preying parties, often engaged in criminal activity. Technological advances commonly utilized in the practice of law, and the risks to unauthorized disclosure of client information they entail, thus require a regulatory shift in the Rules, from avoiding inadvertent disclosure to acknowledging a positive duty to protect confidential information. Put differently, the unique challenge cybersecurity concerns present is not merely coming to terms with technological advancements, which

---

115 Wald, *supra* note 9, at 228.

116 *Id.*

117 Silkenat, *supra* note 2, at 450; *see, e.g.*, MODEL RULES OF PROF'L CONDUCT r. 4.4(b) (AM. BAR ASS'N 2013).

the profession, while reluctant, has done in the past.[118] Rather, it is shifting from a passive regime of avoiding negligent disclosure to an active regime of affirmatively protecting information against parties, some of which engage in criminal activity.

To be clear, the emergence of lawyers' affirmative duty to reasonably protect client information from unauthorized disclosure is not a move toward strict liability. Fully protecting client information from all cyberattacks is not feasible given current available technologies, and even if complete protection was possible, it might so undercut the use of effective technology and be so cost prohibitive as to render it unreasonable. Furthermore, utilizing technology to better serve the needs of clients, and confronting the risks inherent in the use of technology, is and ought to be a joint attorney-client undertaking. As clients reap the benefits of new technologies and are sometimes better positioned as compared to their lawyers to address their risks, there is no reason to impose strict liability on lawyers for the use of technology in the practice of law. Accordingly, lawyers need only take reasonable steps to protect client information. Yet, the Rules' approach to cybersecurity must recognize and effectuate an affirmative duty to reasonably protect clients' information and develop a helpful definition of reasonableness that encompasses an obligation to protect client information from criminal activity. The Rules must clarify that a lawyer not only needs to avoid negligently leaving notes in plain view, but must also protect against theft of one's virtual briefcase.

1. Mandating the Adoption of Appropriate Cybersecurity Plans for All Clients

Lawyers' cybersecurity conduct is underregulated, which likely results in insufficient action to protect client information. Because liability rules and market controls are unlikely to effectively incentivize lawyers to take reasonable action, the Rules must require that lawyers adopt appropriate cybersecurity plans. Revealingly, the ABA's 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."[119] Yet nothing in the Rules imposes a duty on lawyers to develop cybersecurity programs for all clients.

---

118 Toohey, *supra* note 65.

119 ABA CYBERSECURITY RESOLUTION, *supra* note 3 (emphasis added).

To be sure, Comment 18 on Rule 1.6 does state that: "[p]aragraph (c) requires a lawyer *to act competently to safeguard information* relating to the representation of a client against unauthorized access by third parties," and adds that: "[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer *has made reasonable efforts to prevent the access or disclosure*,"[120] arguably indirectly encouraging lawyers to put in place a cybersecurity plan for all clients. After all, "acting competently" and making "reasonable efforts" would seem to require at least implementing a cybersecurity plan. Yet the Rules do not affirmatively require the adoption of such a plan and would appear to tolerate an interpretation that at least in some circumstances the prongs of "acting competently" and making "reasonable efforts" could be satisfied without the implementation of a cybersecurity plan. Indeed, Comment 18 does not specify what constitutes "acting competently" nor "reasonable efforts."[121]

The Rules ought to require that all lawyers maintain an appropriate cybersecurity plan, akin to Comment 3 on Rule 1.7, which mandates the adoption of reasonable conflict-checking procedures.[122] Accordingly, a new Comment X to Rule 1.6 should read:

> [t]o competently safeguard information relating to the representation of a client against unauthorized access by third parties, a lawyer must adopt reasonable procedures, including reasonable cybersecurity measures, appropriate for the size and type of firm and practice, to protect a client's confidential information. Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule.[123]

---

120 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 18.

121 *See* Ezekiel, *supra* note 13, at 658–59 ("These rules generally require the law firms to take 'reasonable efforts,' 'reasonable steps,' or 'reasonable precautions' to avoid unauthorized disclosure, but are unspecific about what such precautions might entail. One rule demands that the precautions taken must "meet[] industry standards," but is unfortunately vague about whether it refers to the standards of the *legal* industry or those of the *Internet data storage* industry.") (internal citations omitted).

122 MODEL RULES OF PROF'L CONDUCT r. 1.7 cmt. 3.

123 The Comment to Rule 1.6 includes two sections, Comments 18 and 19, under the subheadings of "Acting Competently to Preserve Confidentiality." *See id.* The proposed Comment can be added as Comment 18, renumbering current Comments 18 and 19 as 19 and 20 respectively; or as Comment 20 (renumbering current Comment 20 regarding confidentiality duties owed to former clients as Comment 21). Or the proposed Comment can be added to the existing Comment. For a redline of the proposed revisions to the Rules, see Appendix A.

2. Defining "Reasonable Efforts": Reasonable Cybersecurity Measures

Just as Comment 3 on Rule 1.7 has resulted in virtually all law firms employing a conflict-checking software as the first step in detecting conflicts of interest, proposed new Comment X to Rule 1.6 should result in all law firms adopting basic cybersecurity measures, such as employing current virus scanners and firewalls, installing patches and updates, and using cryptographically strong passwords, reasonably replaced from time to time,[124] as the first step in implementing a comprehensive cybersecurity plan. Yet the adoption of basic cybersecurity measures should not be left to chance. Instead, adoption of such basic security measures must be explicitly recognized as a professional requirement for any attorney who stores sensitive client data on an Internet-connected computer.[125] For example, law firms must be expected to demonstrate their system's ability to detect and repel a cyberattack.[126]

Thus, to begin with, "reasonable efforts" must include basic cybersecurity measures such as "robust strategies for identifying, prioritizing, and securing . . . valuable information,"[127] periodical inspection of the firm's operating and information storage systems for signs of cyberattacks and data theft, the use of current virus scanners and firewalls, installing patches and updates, using cryptographically strong passwords, avoiding risky software downloads from the Internet, eschewing the use of public cloud providers or file sharing services for sharing documents, avoiding the use of web-based e-mail services and public Wi-Fi, replacing the default passwords on network hardware, and the adoption of training protocol for firm lawyers and staff, appropriate for the size and practice of the firm, for example, to recognize phishing attacks.[128]

A new Comment Y to Rule 1.6 should read:

> [r]easonable 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

---

124 *See supra* note 29 and accompanying text.
125 *See* Ezekiel, *supra* note 13, at 665.
126 Silkenat, *supra* note 2, at 455.
127 McNerney & Papadopoulos, *supra* note 12, at 1250.
128 *See supra* note 29 and accompanying text.

> 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. *See* Rule 5.1 and 5.3.[129]

An attempt to identify basic cybersecurity measures in the Comment entails two related risks. A closed-list of measures may, over time, be treated as a "check-a-box" procedure for purposes of avoiding discipline, or understood to constitute a safe harbor—in the sense that lawyers who employ these basic cybersecurity measures may never be found to have failed to make "reasonable efforts" to protect their clients' information. To avoid such misapprehension, the Comment should explain that basic cybersecurity measures form but a floor for appropriate cyber conduct, necessary but often insufficient means of satisfying the requirement of "reasonable efforts." Far from constituting a safe harbor, basic measures simply set up a default foundation for "reasonable efforts," which depend on a variety of factors already identified by the Comment. Moreover, the Comment should explicitly state that some circumstances may require the adoption of additional special cybersecurity measures.

Comment Z to Rule 1.6 may accordingly add that:

> [w]hether a lawyer may be required to take additional special security measures to safeguard a client's information, above and beyond basic cybersecurity measures, depends on the circumstances. For example, a lawyer may be required to take special security measures to protect sensitive information related to the representation of a client.[130]

Relatedly, technological advances may, over time, render proposed Comment Y obsolete, a concern compounded by the traditional delay involved in adoption of revisions to the Rules, first at the ABA level and subsequently by states to their respective rules of professional conduct. Indeed, one commentator concludes that given the long delay inherent in Rules revisions, the "ABA and state bar associations have demonstrated that they might not be the best sources of reform in this subject [cybersecurity]."[131] Yet one should not overstate the rate of relevant technological advances, indeed, many of the currently available basic cybersecurity measures, admittedly in more

---

129 See *infra* Appendix A for a redline of the proposed revisions to the Rules. Rules 5.1 and 5.3 ought to be amended respectively to reference proposed Comment Y to Rule 1.6.

130 *Id.*

131 Travis Andrews, *Technological Innovation, The Legal Profession and the Need for Uniform Law*, CHARLOTTE L. REV. (forthcoming 2016) (manuscript at 2), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2684950.

primitive forms, have been available for a few decades now. In any event, lamentable delays in promulgation and revision notwithstanding, the Rules remain the only practical and, therefore, most operative means of correcting for the underregulation of lawyers' cybersecurity conduct, given the ineffectiveness of liability rules and market controls and the distant probability of national cybersecurity legislation, let alone one that would apply to lawyers. If at all, a years-long delay in the promulgation of the Rules and their adoption by the states does not constitute a compelling reason to avoid regulation. Quite the contrary, the delay ought to be addressed by reforming the historical process of promulgation and adoption to ensure that the Rules remain relevant and helpful to lawyers. There is no denying that old political habits die hard, especially at the hands of the ABA House of Delegates and state supreme courts' advisory committees. Yet, failure by the legal profession to effectively regulate itself may result, and in fact has resulted, in increased federal and state legislation undermining the profession's privilege of self-regulation.[132]

Nor would an ABA Formal Opinion be an adequate substitute to proposed Comment Y to Rule 1.6. Ethics opinions, while relatively easier and faster to publish and withdraw, if rendered obsolete, have no binding authority and are therefore inferior to Rules' revisions.[133] Moreover, given the underregulation of lawyer's cybersecurity conduct, ethics opinions will simply not do. The Rules must be revised to send lawyers a credible message, both substantively and symbolically, about the importance of acting affirmatively to protect clients' information. If technology ends up rendering proposed Comment Y obsolete, it can be revised in accordance with evolving cybersecurity knowledge and expertise.

---

132 *See* Daniel R. Coquillette & Judith A. McMorrow, *Zacharias's Prophecy: The Federalization of Legal Ethics*, 48 SAN DIEGO L. REV. 123 (2011) (documenting the federalization of legal ethics); Bruce A. Green, *ABA Ethics Reform from "MDP" to "20/20": Some Cautionary Reflections*, 2009 J. PROF. LAW. 1, 4–7 (2009) (arguing that future reform to the regulation of lawyers may require abandoning the state-based approach); Eli Wald, *Federalizing Legal Ethics, Nationalizing Law Practice and the Future of the American Legal Profession in a Global Age*, 48 SAN DIEGO L. REV. 489 (2011); Fred C. Zacharias, *Federalizing Legal Ethics*, 73 TEX. L. REV. 335 (1994); *see also* Ted Schneyer, *Professional Discipline in 2050: A Look Back*, 60 FORDHAM L. REV. 125, 127 (1991) (predicting the adoption of a "Federal Code of Lawyering"). Of course, states may act independent of the ongoing federalization of legal ethics and regulate the practice of law within their jurisdictions. *See, e.g.*, CAL. BUS. & PROF. CODE § 6000 (West 2016).

133 *See* Peter A. Joy, *Making Ethics Opinions Meaningful: Toward More Effective Regulation of Lawyers' Conduct*, 15 GEO. J. LEGAL ETHICS 313, 317–19 (2002).

3. "Reasonable Efforts" Further Construed

To further clarify that basic cybersecurity measures merely define a floor rather than a ceiling for "reasonable efforts," the Comment to Rule 1.6 must spell out the meaning of "reasonable efforts" beyond such basic steps. Comment 18 already helps construe "reasonable efforts," stating in relevant part:

> [f]actors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[134]

Comment 19 adds that:

> [w]hen transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use *special security measures* if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.[135]

The Comment, however, does not define the term "special security measures," except indirectly by using language similar to the one used in ABA Formal Opinion 99-413 on encryption of confidential information.[136] Instead, the Comment can provide examples of "special security measures," such as the use of encryption to protect sensitive client information and attorney-client communications.[137]

Next, the Comment may explicitly state that a lawyer who fails to take the most basic security precautions violates Rule 1.6(c), even if the client's information was accessed by a third party criminally. In other words, the Comment should state that the criminal conduct of third parties does not constitute a safe harbor to lawyers who fail to make "reasonable efforts" to protect the information. Historically, the Rules made attorneys liable for their own conduct, for example, inadvertently disclosing

---

134 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 2013).
135 *Id.* r. 1.6 cmt. 19 (emphasis added).
136 *See* ABA Comm. on Ethics & Prof'l Responsibility, *supra* note 84.
137 See proposed Comment U, Appendix A.

confidential client information, but not for the criminal actions of third parties. "This view," explains Alan Ezekiel, "that attorneys are not responsible for violations of client privacy that flow from criminal misconduct by third parties may have been informed by the evolution of legal standards regarding the use of mobile phones."[138] Whereas early ethics opinions in the 1990s suggested that attorneys might violate rules of professional conduct by discussing private client information on mobile phones because outsiders could overhear the conversations, later opinions reflected the view that "the Electronic Communications Privacy Act (which criminalized interception of wireless telephone conversations) created a reasonable expectation of privacy on a mobile phone, and thus the attorney could discuss client matters on a mobile phone without violating any ethical standards."[139] Importantly, "[t]he fact that an outsider might be able to overhear the conversation was irrelevant," adds Ezekiel, "because the outsider would thereby be committing a felony."[140]

Similarly, because "[a] hacker would be committing a felonious violation of the Computer Fraud and Abuse Act by accessing client records without authorization,"[141] Comment 19's statement that the duty to protect client information "does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy"[142] can be read to suggest that an attorney who fails to prevent unauthorized criminal access to client information is not acting unreasonably. "But," asked Ezekiel compellingly, "should the fact that hacking is illegal excuse an attorney who fails to take even the most basic security precautions in an era of widespread data theft?"[143]

Of course, that a third party commits a crime to access client information is relevant in terms of determining the consequences for the client. For example, because the attorney-client privilege belongs to the client, only the behavior of the client—holder of the privilege—or the client's lawyer-agent can waive it. Therefore, in most jurisdictions, intercepted communications are still privileged, meaning that client information stolen from the lawyer would nonetheless continue to be privileged.[144] Such attempts to mitigate the consequences of information theft for

---

138 Ezekiel, *supra* note 13, at 659.
139 *Id.*
140 *Id.* at 659–60.
141 *Id.*
142 MODEL RULES OF PROF'L CONDUCT r. 1.6 cmt. 19 (AM. BAR ASS'N 2013).
143 Ezekiel, *supra* note 13, at 660.
144 Hughes, *supra* note 26, at 417–18.

victim-clients ought not, however, negate the misconduct of an attorney who fails to utilize basic cybersecurity measures to protect client information.

Thus, in addition to offering examples of "special security measures" and the circumstances which warrant them, the Comment to Rule 1.6 must clearly state that a third party's criminal activity accessing clients' information does not negate the responsibility of a lawyer who fails to take reasonable cybersecurity measures on behalf of clients. Comment V to Rule 1.6 may accordingly add that:

> [t]he unauthorized access to information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. However, an unauthorized access to information relating to the representation of a client may constitute a violation of paragraph (c) if the lawyer has not made reasonable efforts to prevent the access, even if a third party accessed the information unlawfully.[145]

4. Disclosure of Cyberattacks and Data Theft to Clients

The Rules do not impose a general duty on lawyers to advise clients when their information has been compromised in a cyberattack, let alone that the law firm was or is under attack.[146] Rule 1.4(a)(3) only requires lawyers to "keep the client reasonably informed about the status of the matter," which Comment 3 explains means advising clients regarding "significant developments affecting the . . . substance of the representation."[147] Yet, as we have seen, because often the identity of the attacker, the nature of the information compromised, and the extent of the damage to the client are unknown, a lawyer may not be in a position to conclude that the cyberattack or data theft constitute "a significant development" as opposed to a mere development, and so Rule 1.4(a)(3) is not triggered. Similarly, the inherent uncertainty often surrounding cyberattacks means that Rule 1.4(b)'s admonition for lawyers to "explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation"[148] may not be triggered because the impact on the matter at hand may be less than clear to the lawyer.

---

145 For a redline of the proposed revisions to the Rules, see Appendix A.

146 *See supra* Section III.A.

147 MODEL RULES OF PROF'L CONDUCT r. 1.4(a)(3).

148 *Id.* r. 1.4(b).

This prevailing interpretation of Rule 1.4 finds some support in the recent rule amendments regarding cybersecurity. Comment 18 on Rule 1.6 states in relevant part that:

> [w]hether 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.[149]

Read narrowly, the Comment merely states the obvious, namely, that the Rules never, and do not in the case of cybersecurity, purport to construe "other law" such as state and federal laws that may or may not impose additional duties on lawyers. Yet the Comment may also imply or may be read by some lawyers to suggest that notification requirements to clients upon the loss or unauthorized access to their information are beyond the scope of the Rules.

The better interpretation of Rule 1.4, however, is that it does impose an affirmative duty on lawyers to notify clients when their confidential information has been compromised, even when the consequences and impact of the attacks on clients' information fall short of the "significant development" threshold of Rule 1.4(a)(3) or the duty to explain a matter and the means by which it is to be pursued to a client per 1.4(b). To see why imposing a disclosure duty is warranted, recall that Rule 1.4(a)(3), as construed by Comment 3, does impose a duty on lawyers to advise clients regarding a significant development affecting the representation. The Rule assumes that in most circumstance a lawyer would be able to determine whether a particular development is either significant (and therefore triggers 1.4(a)(3)) or less than significant (such that 1.4(a)(3) is not triggered). Cyberattacks, however, are an example of a circumstance possibly not anticipated by the Rules—one in which inherent uncertainty prevents a lawyer from reasonably concluding whether a development affecting the matter is significant or not. In such a case, lawyers as agents and fiduciaries of clients must err on the side of caution and advise their principals-clients of the development.[150] That is, in the face

---

149 *Id.* r. 1.6 cmt. 18 (emphasis added).

150 Elsewhere, I argue that Rule 1.4 should be revised and/or interpreted to mean that lawyers must advise clients regarding all material developments regarding the representation. *See* Eli Wald, *Taking Attorney-Client Communications (and Therefore Clients) Seriously*, 42 U.S.F. L. REV. 747, 789–91 (2008). Inherent uncertainty regarding cyberattacks may leave lawyers unable to determine whether an attack constitutes a material development affecting the representation. Taking attorney-client communications, and therefore clients, seriously dictates that when faced with such inherent uncertainty, lawyers must err on the side of disclosing more rather than less information relating to

of inherent uncertainty regarding the impact of cyberattacks and whether client information has been compromised, a question arises as to whether clients should know more or less about the development. Because clients are the principals in the attorney-client relationship and lawyers are mere agents-fiduciaries, it appears that in the face of inherent uncertainty, lawyers must err on the side of more, rather than less, disclosure to clients. This interpretation is especially compelling in the context of cyberattacks, in which clients, as opposed to lawyers, would often be in the best position to assess the impact of and respond to cyberattacks.[151]

Acknowledging that in general, lawyers must tell clients more about compromised client information requires detailing when lawyers must communicate with clients—identifying the specific triggering event for disclosure—and how they ought to go about discussing cyberattacks and their consequences with clients. In this regard, the Rules may learn from existing states' personal information data breach notification statutes.[152] For example, California Civil Code section 1798.82(a) states that:

> (a) A person or business . . . that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a [person] whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay . . . .[153]

California's statutory notification provision is noteworthy in at least two ways. First, while it imposes a mandatory duty to notify customers,[154] the duty is triggered only when the protected information was or is reasonably believed to have been compromised.[155] The provision, to be clear, does not impose a notification duty when a cybersecurity system storing protected information is under a cyberattack, presumably because such a trigger would reveal little to customers if the system was able to thwart the attack. Rather, notification is mandated either when protected information was compromised, or, in the face of some uncertainty, when it is reasonable to assume that the protected information has been compromised. Second, the statute only requires notification when a person's "*unencrypted* personal

---

the representation to clients. *Id.* at 748–50.

151 *See* Goldberg, *supra* note 25, at 540–41.

152 McNerney & Papadopoulos, *supra* note 12, at 1254–56.

153 CAL. CIV. CODE § 1798.82(a) (West 2016).

154 *Id.* ("shall disclose a breach of the security of the system").

155 *Id.* ("whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person").

information was, or is reasonably believed to have been, acquired by an unauthorized person."[156] That is, because the statute only requires notification when unencrypted information was or is reasonably believed to have been compromised, arguably encryption of the information provides a practical safe harbor and negates the need to disclose a breach.

The statutory experience thus suggests two models the Rules can follow. Akin to California's notification apparatus, a modest revision to the Rules can require disclosure to clients only when a client's confidential information has been or is reasonably believed to have been compromised, and only if the confidential information was not reasonably protected, such that if a lawyer reasonably protects the information (via encryption or otherwise) no disclosure to clients would be mandated. For example, the Rules may be amended to state that:

> A lawyer who stores (or employs a third party provider to store) information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose unreasonably protected confidential information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.

Such a disclosure provision would naturally follow and complement the above proposals requiring all lawyers to adopt cybersecurity plans for all their clients and to make reasonable efforts to protect clients' confidential information. Lawyers who take these two steps would, practically speaking, have no duty to report to clients when their information has been or is reasonably believed to have been compromised because they would be covered by a safe harbor of reasonableness.

In the alternative, the Rules may adopt the triggering event of the personal information notification statutes—information that was or is reasonably believed to have been compromised—without excusing disclosure to clients even when the lawyer did make reasonable efforts to protect the information. Comment W to Rule 1.4 should read:

> A lawyer who stores (or employs a third party provider to store) information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose confidential information was, or is reasonably believed to have been, acquired by

---

156 *Id.* (emphasis added).

> an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.[157]

The latter approach appears to be warranted in the context of the attorney-client relationship. When a client's confidential information was or is reasonably believed to have been compromised, clients must be advised, even if the lawyer did make reasonable efforts to protect the information. One might argue that when a lawyer has made reasonable efforts to protect the information, imposing a mandatory duty on lawyers to advise clients that their information was, or is, reasonably believed to have been compromised is likely to be ineffective—burdening the client with irrelevant information, with possible distinct adverse consequences, such as chilling or eroding the attorney-client relationship. Put differently, would not mandating adoption of cybersecurity plans and spelling out reasonable efforts be enough? If these provisions end up ensuring reasonable conduct by lawyers, why force disclosure and risk clients developing "notice fatigue"? Would not clients be content with lawyers' adoption of reasonable efforts? If nothing else could have been reasonably done by lawyers, why tire the clients with additional disclosures?

These objections, however, must be rejected for three related reasons. First, they smack of lawyers' self-interest at the expense of clients, the very concern about and criticism of the Rules to which lawyers ought to be sensitive.[158] No doubt, reporting to a client that the client's confidential information was or is reasonably believed to have been compromised is likely to be awkward to the lawyer,[159] but that is not in and of itself a legitimate ground a lawyer should be able to invoke to avoid disclosing information to the client.

Second, recall that this Article advocates a revision to the Comment to Rule 1.6, pursuant to which "a lawyer must adopt reasonable procedures . . . appropriate for the size and type of firm and practice, to protect a client's information," including reasonable cybersecurity procedures.[160] With such a cybersecurity plan in place, a lawyer's communication to a client regarding a breach and compromised information following a cyberattack is

---

157 For a redline of the proposed revisions to the Rules, see Appendix A, proposed Comment W to Rule 1.4.

158 *See supra* notes 45–46 and accompanying text.

159 Recall that if a cyberattack has in fact resulted in disclosure of a client's material confidential information, then even a traditional reading of 1.4(a)(3) and 1.4(b) will mandate disclosure to the client. *See* MODEL RULES OF PROF'L CONDUCT r. 1.4(a)(3), 1.4(b) (AM. BAR ASS'N 2013).

160 *See supra* note 123 and accompanying text.

unlikely to chill the attorney-client relationship, because a lawyer would be able to cheaply and effectively explain to the client the reasonable efforts the law firm made to protect the client's information, and the inherent uncertainty surrounding the cyberattack, notwithstanding the reasonable security measures undertaken. Indeed, it is the current state of technology that prevents lawyers (and others) from stopping all cyberattacks and reasonable clients should be able to understand and accept a lawyer's reasonable conduct in the face of technological limitations and uncertainty.

Finally, any interpretation second-guessing disclosing information to clients when confidential information was or is reasonably believed to have been compromised on the ground that clients may not understand it or will be fatigued smacks of lawyers' paternalism vis-à-vis clients, inappropriate in the attorney-client relationship.[161] As I explain elsewhere, "for lawyers to assume that clients are unable to comprehend and appreciate the consequences and meaning of complex . . . information, even when offered a detailed explanation . . . would constitute unacceptable paternalistic withholding of material information."[162] The U.S. Supreme Court, in its landmark decision, *Basic, Inc. v. Levinson*,[163] construed the term "material" in securities law. It held that to address inherent uncertainty by not disclosing material information to clients amounts to assuming that clients are

> nitwits, unable to appreciate—even when told—that [cybersecurity measures] are risky propositions . . . . Disclosure, and not paternalistic withholding of accurate information, is the [desirable] policy . . . . The role of the materiality requirement is not to 'attribute to [clients] a child-like simplicity, an inability to grasp the probabilistic significance of [cybersecurity measures]' . . . but to filter out essentially useless information that a reasonable [client] would not consider significant, even as part of a larger 'mix' of factors to consider in making his . . . decision[164]

regarding the attorney-client relationship.

Moreover, fatigue assumes that clients would know and may not care or become indifferent about security breaches. Yet the assumption seems inapplicable here. Currently, clients do not usually learn about, and are unlikely to be indifferent about breaches regarding their confidential information. For the same reason, mandating disclosure to clients only when the unauthorized access of confidential information is likely to have a

---

161 MODEL RULES OF PROF'L CONDUCT r. 1.2(a).
162 Wald, *supra* note 150, at 795.
163 Basic Inc. v. Levinson, 485 U.S. 224 (1988).
164 *Id.* at 234; *see also* Wald, *supra* note 150, at 795–96.

prejudicial impact on their representation would not suffice. Just as the inherent uncertainty surrounding cyberattacks often precludes lawyers from concluding that a breach of confidential information constitutes a "significant development" mandating disclosure to clients, the same uncertainty will likely prevent lawyers from concluding that a breach has a prejudicial impact on clients' representation. Because a reasonable client would like to know when her confidential information was, or is, reasonably believed to have been accessed by an unauthorized party, a lawyer must disclose accordingly.

Mandating disclosure to clients when confidential information was, or is, reasonably believed to have been compromised has one additional important benefit. Disclosure would, in turn, enable clients to sanction lawyers who fail to put in place "reasonable efforts" to protect their confidential information and reward lawyers who do make reasonable efforts to protect confidential information. Put differently, the adoption of a rule of professional conduct mandating disclosure of cybersecurity information to clients would allow clients to exercise market controls over lawyers, further addressing the underregulation of lawyers' cybersecurity conduct. Finally, even if lawyers do make reasonable efforts to protect confidential information, a disclosure duty would result in more conversations with clients about cybersecurity, allowing clients to participate on an informed basis regarding the cyber means by which their objectives are to be pursued.

CONCLUSION

The inherent uncertainty often surrounding cyberattacks on law firms—who specifically perpetrated the attack, what information was stolen or compromised, and what damage, if any, did a client suffer as a result of the attack—renders liability rules, such as malpractice suits, and market controls, such as being fired by a client, ineffective in regulating lawyers' cybersecurity conduct. The Rules thus have an opportunity to play a meaningful role in informing and guiding the conduct of underregulated lawyers, by requiring lawyers to adopt and implement cybersecurity plans for all clients, defining the meaning of "reasonable efforts" necessary to prevent the unauthorized disclosure or access to information relating to the representation of a client, and by mandating disclosure to clients when their confidential information was, or is, reasonably believed to have been accessed by an unauthorized party.

Appendix A: Proposed Revisions to the Rules

Proposed revisions to the Rules are italicized.

Comment on Rule 1.6

Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

[X] To competently safeguard information relating to the representation of a client against unauthorized access by third parties, a lawyer must adopt reasonable procedures, including reasonable cybersecurity measures, appropriate for the size and type of firm and practice, to protect a client's confidential information. Ignorance caused by a failure to institute such procedures will not excuse a lawyer's violation of this Rule.

The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure.

[Y] Reasonable efforts to prevent the inadvertent or unauthorized disclosure of 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. See Rule 5.1 and 5.3.

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

additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

[Z] Whether a lawyer may be required to take additional special security measures to safeguard a client's information, above and beyond basic cybersecurity measures, depends on the circumstances. For example, a lawyer may be required to take special security measures to protect sensitive information related to the representation of a client.

A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules, *but see Rule 1.4, Comment [U].* For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy.

[U] Special security measures may include encryption of attorney-client communications or password-protecting information relating to the representation of a client on the lawyer's or law firm's information storage system.

Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws

that govern data privacy, is beyond the scope of these Rules, *but see Rule 1.4, Comment [3].*

[V] The unauthorized access to information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. However, an unauthorized access to information relating to the representation of a client may constitute a violation of paragraph (c) if the lawyer has not made reasonable efforts to prevent the access, even if a third party accessed the information unlawfully.

Comment on Rule 1.4

Communicating with Client

[3] Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations — depending on both the importance of the action under consideration and the feasibility of consulting with the client — this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[W] A lawyer who stores (or employs a third party provider to store) *information related to the representation of a client, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a client, whose confidential information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay.*