Washington Law Review

Volume 99 | Number 3

10-1-2024

Client Confidentiality as Data Security

Jonah E. Perlin
Georgetown University Law Center

CLIENT CONFIDENTIALITY AS DATA SECURITY

Jonah E. Perlin*

Abstract: The duty of confidentiality has been a cornerstone of the attorney-client relationship for more than four centuries. Historically, this duty was not difficult to discharge. All a lawyer had to do to comply was not affirmatively share client information in public without consent. But that has all changed. The same technologies that provide unprecedented benefits of authorized access by lawyers and their clients create unprecedented risks of unauthorized access by others. As a result, although the duty of confidentiality was once synonymous with a duty to keep client confidences secret, today the duty necessitates that lawyers keep client confidences secure as well.

This critical shift did not go entirely unnoticed by the legal profession. In 2012, the American Bar Association adopted Model Rule of Professional Conduct 1.6(c) which requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to," client confidences. This new rule had good intentions and was eventually adopted in some form by every state bar. Yet it has proven ineffective at protecting clients and difficult, if not impossible, to execute for lawyers. Worse, in the more than a decade since its adoption there has not been a single published disciplinary action for violating this duty in the digital context. Not one.

After telling the story of the legal profession's adoption of a duty of data security and the shortcomings with the current approach to that duty, this Article seeks to outline its next chapter. Specifically, it argues that the lawyer's duty of data security should not focus exclusively on the regulation of technological safeguards to prevent breaches and should focus instead on regulating the processes that lawyers must take to mitigate harm from potential breaches and the people that lawyers must consult when making data security decisions. This approach draws inspiration not only from professional responsibility scholarship but also from data security best practices from outside the legal profession that can help guide lawyers, protect clients, and incentivize enforcement by state bars despite constant technological innovation.

---

*Associate Professor of Law, Legal Practice, Georgetown University Law Center. I would like to thank Colin Ahern, Erin Carroll, Catherine (Cassie) Christopher, Sara Colangelo, Brian Farkas, Michael Frisch, Eun Hee Han, Robert Jossen, Jon Lee, Amanda Levendowski, Renee Knake Jefferson, Kirk Nahra, Paul Ohm, Dyane O'Leary, Eloise Pasachoff, Debra Perlin, Nancy Rapoport, Joe Regalia, Mitt Regan, Sarah J. Schendel, Rima Sirota, Neel Sukhatme, Gabriel Teninbaum, Ed Walters, and the participants and organizers of the 2023 AALS Professional Responsibility Section's New Voices in Professional Responsibility Panel for their helpful thoughts and suggestions at various stages of the writing of this Article. For research assistance, I am extremely grateful to Jada Cushnie, Katharine Kuchinski, Laixin Li, Annie Moody, Taylor-Ryan Nedd, Lauren Wells, Max Van Zile, Andrew Yablonsky, and Michelle Zhang. Finally, I also want to thank the staff of the *Washington Law Review* for their careful editorial work.

INTRODUCTION

The adoption of new technologies has consistently changed the legal profession. Among these changes, one of the most stark has been and continues to be technology's impact on the longstanding duty of lawyer-client confidentiality. Client confidences once stored in file cabinets, briefcases, and locked offices, increasingly are now stored instead on laptop computers, mobile phones, and third-party servers. This new digital reality brings with it significant benefits to the legal profession. Lawyers are now able to more efficiently and effectively assess, manipulate, and review client documents and data that are orders of magnitude more

voluminous than they were even a generation ago.[1] Beyond that, cloud-based digital communication and storage allow lawyers today to create and access client documents and communicate with clients at speeds once unimaginable anytime, anywhere, and on any device.[2] Not only does this facilitate an unprecedented level of client service, but it also allows lawyers greater flexibility in where, when, and how they practice.[3]

The challenge is that the very same technologies that provide these unprecedented benefits of authorized access by lawyers and their clients create unprecedented risks of unauthorized access by others. More specifically, storing client documents in the cloud and communicating with clients digitally creates a greater risk of accidental disclosure such as sharing the wrong link with a client or sending a confidential e-mail to the wrong recipient.[4] It also creates a significantly greater risk of being targeted by hackers who see the digital data kept by lawyers as a treasure trove.[5] These bad actors have come to understand lawyers and law firms as the unguarded side door to the well-guarded front door of digital

1. RICHARD SUSSKIND, TOMORROW'S LAWYERS: AN INTRODUCTION TO YOUR FUTURE 11 (3d ed. 2023).

2. *See, e.g.*, Stuart L. Pardau & Blake Edwards, *The Ethical Implications of Cloud Computing For Lawyers*, 31 J. MARSHALL J. INFO. TECH. & PRIV. L. 69, 70 (2014); *Why Cloud-Based Legal Work Is Critical for Success*, THOMSON REUTERS LAW BLOG (Jan. 24, 2023), https://legal.thomsonreuters.com/blog/why-the-cloud-is-critical-to-your-firms-success/ [https://perma.cc/H8A6-6EGL].

3. The benefits of this flexibility of location were well-known prior to the precipitous shift to remote lawyering during the COVID-19 pandemic. *See* Eliu Mendez, *Dropping Dropbox in Your Law Practice to Maintain Your Duty of Confidentiality*, 36 CAMPBELL L. REV. 175, 178 (2013) ("Cloud computing provides attorneys with remote accessibility to any client file, document, folder, or application from anywhere with an [i]nternet connection. In fact, forty-one percent of users cite remote accessibility as the primary reason for cloud use."). But it is no exaggeration to say that during the pandemic, remote access to confidential client data and the ability to communicate with clients digitally became mission critical to the practice of law. And in the pandemic's wake, neither the technological tools nor the client services and lifestyles that they facilitated are going away. *See* Ethan S. Burger, *Professional Responsibility, Legal Malpractice, Cybersecurity, and Cyber-Insurance in the COVID-19 Era*, 11 ST. MARY'S J. ON LEGAL MALPRACTICE & ETHICS 234, 237 (2021) ("The COVID-19 pandemic . . . has dramatically, and perhaps permanently, changed how most U.S. lawyers and their law firms deliver legal services.").

4. *See* THE ABA CYBERSECURITY HANDBOOK 431 (Jill D. Rhodes, Robert S. Litt & Paul Rosenzweig eds., 3d ed. 2022); Ben Collins, *After Alex Jones' lawyers accidentally leak years of emails, Infowars financial documents are revealed in court*, NBC NEWS (Aug. 3, 2022), https://www.nbcnews.com/news/us-news/alex-jones-lawyers-accidentally-leak-years-emails-infowars-financial-d-rcna41378 [https://perma.cc/8A22-GJY2].

5. *See, e.g.*, Sharon D. Nelson, John W. Simek & Michael C. Maschke, *Law Firm Data Breaches Surge In 2023*, ABOVE THE LAW (Aug. 1, 2023), https://abovethelaw.com/2023/08/law-firm-data-breaches-surge-in-2023/ [https://perma.cc/VR3E-L9AV].

security that clients spend significant time and money to protect.[6] As one commentator aptly put it, the legal profession is "the soft underbelly of American cyber security."[7] As a result, protecting client confidentiality is no longer just about data *secrecy*, it is equally about data *security* as well.

More than two decades ago—largely in response to concerns about whether using unencrypted e-mail to communicate with clients violated the professional duty of confidentiality[8]—the American Bar Association (ABA) adopted a non-binding comment to the *Model Rules of Professional Conduct* encouraging lawyers to "act competently to safeguard information relating to the representation of a client against . . . inadvertent or unauthorized disclosure . . . [and] take reasonable precautions to prevent the information from coming into the hands of unintended recipients."[9] In 2012, the ABA then took the even more significant step of codifying this non-binding guidance into the duty of confidentiality's binding text.[10] New subsection (c) of Model Rule 1.6 requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[11] Two new comments accompanied the adoption of this new subsection, which identify specific factors for lawyers to consider when taking these "reasonable efforts." [12] These non-binding and non-exclusive factors focus on balancing the need for technological safeguards to prevent disclosure on the one hand with the difficulty and cost of employing those safeguards on the other.[13] In more recent years, the ABA has continued to define, refine, and arguably

---

6. *See* Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19 CHAP. L. REV. 501, 506 (2016) (discussing the reasons that lawyers are targets of hackers); ABA Cybersecurity Legal Task Force, *Report To The House Of Delegates: Resolution 109* (2014) [hereinafter ABA Resolution 109], http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resolutions/2014_hod_annual_meeting_109.authcheckdam.pdf [http://perma.cc/NS7C-JXS7] ("Lawyers and law firms are facing unprecedented challenges from the widespread use of electronic records and mobile devices.").

7. Joe Patrice, *When Luddites Handle Cyber Security, You End Up With American Law Firms*, ABOVE THE LAW (Feb. 6, 2013), https://abovethelaw.com/2013/02/when-luddites-handle-cyber-security-you-end-up-with-american-law-firms/ [https://perma.cc/9QTJ-RA5Y].

8. *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017).

9. *See* MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N, Draft 2000) https://www.americanbar.org/groups/professional_responsibility/policy/ethics_2000_commission/e2k_report_home/.

10. MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 2012).

11. *Id.*

12. *Id.* at cmts. 18 & 19.

13. *Id.*

expand these duties in Formal Opinions and in its comprehensive *Cybersecurity Handbook*, which is now in its Third Edition.[14]

State bars are, of course, not required to adopt specific ABA model rules.[15] Nevertheless, the voluntary adoption of Model Rule 1.6(c)'s approach to the lawyer's duty of confidentiality has been staggering.[16] In fact, every state bar has cited approvingly to the "reasonable efforts" approach described in Model Rule 1.6(c) with forty-four jurisdictions adopting the verbatim text of Model Rule 1.6(c), the comments to Model Rule 1.6 that preceded it, or both.[17]

Yet despite its mass adoption this approach has fallen short in several critical ways. First, the current approach is ineffective at actually protecting client confidences.[18] Despite this seemingly robust duty of data security, unauthorized and accidental access and disclosure of client confidences continue to occur at an alarming rate. More than one in four lawyers report suffering a data breach and roughly one in forty data breaches worldwide occur in the legal and insurance industries.[19] Each month seems to bring yet another high-profile data security failure in the legal profession. These failures are not limited to a particular type of law firm or practice area.[20] Every lawyer is a potential target: private law firms and public law departments; big law firms and small; US-based and international; plaintiff-side and defense; transactional and litigation.[21]

Second, lawyers do not have the necessary tools to faithfully and efficiently execute this duty.[22] Under the current approach, individual attorneys are required to "make reasonable efforts to prevent inadvertent

---

14. *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017); THE ABA CYBERSECURITY HANDBOOK, *supra* note 4.

15. *See* Bruce A. Green, *Whose Rules of Professional Conduct Should Govern Lawyers in Federal Court and How Should the Rules Be Created?*, 64 GEO. WASH. L. REV. 460, 461–62 (1996).

16. *See infra* Appx. A.

17. *See infra* Appx. A.

18. *See infra* section II.A.

19. *See* Sam Skolnik, Skye Witley & Olivia Cohen, *Law Firm Cyberattacks Grow, Putting Operations in Legal Peril*, BLOOMBERG LAW (July 7, 2023), https://news.bloomberglaw.com/business-and-practice/law-firm-cyberattacks-grow-putting-operations-in-legal-peril [https://perma.cc/XG3Y-CQW8].

20. *See* John Simek, *2022 Cybersecurity TechReport*, AM. BAR ASS'N (Nov. 29, 2022), https://www.americanbar.org/groups/law_practice/resources/tech-report/2022/cybersecurity/ [https://perma.cc/9YD2-ERBL] ("We can't seem to go a single day without hearing about some sort of security event such as a ransomware attack, data breach, newly discovered vulnerability, or some misuse of our information.").

21. *See, e.g.*, Wald, *supra* note 6, at 504 ("Different types of law firms offer different types of potential value to hackers in terms of the confidential client information they store."); ABA Resolution 109, *supra* note 6 ("Both large and small law firms have been the target of hacker attacks in the U.S. as well as abroad.").

22. *See infra* section II.B.

or unauthorized disclosure . . . or . . . access" by balancing the likely effectiveness of particular technological "safeguards" against the cost and difficulty of implementing those technological safeguards given the specific sensitivity of the client confidences at issue.[23] But lawyers do not have the requisite technological expertise to make these assessments.[24] Even if they did, lawyers rarely have sufficient knowledge of the sensitivity of the client confidences that they hold or the risk tolerances and cost preferences of their clients.[25] And even if they had this knowledge, lawyers simply do not have the time to engage in a multi-factor balancing test for each and every piece of confidential client information that they learn or receive. In other words, the current approach sees the lawyer's duty of data security as a technological problem (unauthorized and accidental access and disclosure) with a technological solution (choosing the "right" technologies and digital safeguards to prevent this access). But lawyers simply do not have the tools to solve the problem in this way. It should come as no surprise, therefore, that more than 60% of respondents to the 2021 *ABA Cloud Computing Survey* stated that they had concerns about confidentiality resulting from the use of cloud-based technology.[26]

Third, the current approach to the duty of data security has proven entirely unenforceable by state bars.[27] There are ample examples of unauthorized access and disclosures of confidential information by lawyers and law firms (including many recent and well publicized examples of high-profile lawyers and high-profile clients).[28] Yet a comprehensive search of published state bar association disciplinary decisions turns up *not a single example* of an attorney in any state in the past twenty years being sanctioned for failing to take these "reasonable efforts" in the digital context.[29] Of course, enforcement by state bars is not the sole metric of success for the *Model Rules of Professional Conduct*. The *Rules*, for example, can impact the standard of care in malpractice claims.[30] But this complete lack of enforcement by state bars eliminates

23. MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 2012).

24. *See infra* section II.B.

25. *See infra* section II.B.

26. *See* Dennis M. Kennedy, *2021 Cloud Computing*, ABA TECHREPORT ARCHIVE (Nov. 10, 2021), https://www.americanbar.org/groups/law_practice/resources/tech-report/archive/cloud-computing1/ [https://perma.cc/AV27-UCA6].

27. *See infra* section II.C.

28. *See infra* section II.A and accompanying footnotes.

29. *See infra* section II.C (describing the methodology used to reach this conclusion).

30. *See* Kathleen J. McKee, *Admissibility and Effect of Evidence of Professional Ethics Rules in Legal Malpractice Action*, 50 A.L.R.5th 301 (1997) ("Although it is generally recognized that the

(or at least softens) any perceived deterrent effect of the current approach. It also short-circuits the creation of any sort of common law about what "reasonable efforts" mean in different practice areas and contexts.

Ultimately, the expansion of the lawyer's duty of confidentiality beyond protecting against intentional disclosures was an important innovation consistent with the prevailing wisdom of the time it was adopted. But data security challenges have simply outpaced the legal profession's solutions.[31] Today's lawyers are, at best, stuck with a standard that is unclear, amorphous, and burdensome. At worst, this duty of data security encourages lawyers either to ignore the rules altogether (as we know many do[32]) or to make ineffective and costly choices about data security that do not actually help clients out of a misplaced fear of violating their professional duties. It is beyond time to update the legal profession's approach to the lawyer's duty of confidentiality.

This Article proposes just such a new approach. It proceeds in three parts. After surveying the historical shift from lawyer-client confidentiality as a duty exclusively focused on data secrecy to one also focused on data security in Part I and cataloging the specific challenges with this current approach to the lawyer's duty of data security in Part II, it advocates in Part III for a new approach. Specifically, it argues for a shift away from the profession's current focus on choosing the right technologies and employing reasonable technological safeguards to prevent breaches in favor of an approach centered instead on regulating the ways that lawyers mitigate harm from data security breaches regardless of the specific technologies that lawyers use or their level of technological sophistication.

Under this new approach, lawyers would no longer be required by the ethical rules to simply ask questions about which specific security technologies they can and must use—questions which the profession concedes have no single correct answer.[33] Instead, it argues that compliance with this duty should focus on the specific *processes* that lawyers take to mitigate harm from unauthorized and accidental access of

---

intent of professional ethical codes is to establish a disciplinary remedy rather than to create civil liability, many courts have determined that pertinent ethical standards are admissible as evidence relevant to the standard of care in legal malpractice actions along with other facts and circumstances (§ 3). Professional ethical codes, courts agree, help define an attorney's duty by establishing norms of required professional conduct.").

31. *See infra* section II.A.

32. *See* Kennedy, *supra* note 26 (bemoaning the extreme lack of security measures taken by lawyers as reflected on the ABA 2021 Cloud Computing Survey).

33. ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017) ("[I]t is beyond the scope of an ethics opinion to specify the reasonable steps that lawyers should take under any given set of facts. . . .").

client data and the *people* with whom individual lawyers should be required to consult when making data security decisions. This approach draws on the work of professional responsibility scholars who have long recognized that the current approach is not without many shortcomings.[34] It also takes inspiration from the richly theorized and battle-tested data security frameworks outlined in interdisciplinary scholarship, government regulations, and industry best practices.

To be clear, the goal of this proposal is not to make the duty of confidentiality more amorphous, arduous, or costly. Nor is this an argument for the replacement of a flexible reasonableness approach with a rigid "checklist" or strict liability approach to the duty of confidentiality. To the contrary, although the legal profession is fighting a losing battle to prevent unauthorized and accidental disclosures, data security scholars have long recognized that, "[i]n most cases, it is a poor policy choice for an organization to have the strongest possible security because the tradeoffs are too significant"[35] and "checklists that look good on paper end up being poor in practice."[36] The new approach for which it advocates instead seeks to define the duty of data security in a more practical and effective way that helps lawyers from across the profession walk the fine lines between access and harm and between risk and cost.

To be sure, crafting professional data security standards is no easy task. In data security "there are no absolute answers,"[37] there is only "a delicate dance between technology and people."[38] Moreover, with each new technological innovation comes new data security concerns and considerations.[39] From the increased use of legal technology generally to the recent adoption of generative AI more specifically,[40] "the future threats and risks" related to the lawyer's duty of confidentiality are "as large as our imagination can make them, and larger."[41]

---

34. *See infra* section II.A.

35. DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY LAW FAILS AND HOW TO IMPROVE IT 11 (2022).

36. *Id.* at 196.

37. *Id.* at 11.

38. *Id.*

39. *See* Isha Marathe, *"Data Is the Hot Potato," Attorneys Say, as Leaks and Disclosures Soar in 2022*, LAW.COM (Dec. 9, 2022), https://www.law.com/legaltechnews/2022/12/09/data-is-the-hot-potato-attorneys-say-as-leaks-and-disclosures-soar-in-2022/ [https://perma.cc/24AL-PRBY].

40. *See* Andrew M. Perlman, *The Legal Ethics of Generative AI*, 57 SUFFOLK L. REV. (forthcoming 2024). Many states have already issued specific guidance relating to the use of generative AI that references Model Rule of Professional Conduct 1.6 and its state law analogs. *See, e.g.*, Jim Ash, *Board of Governors Adopts Ethics Guidelines for Generative AI Use*, FLA. BAR NEWS (Jan. 23, 2024), https://www.floridabar.org/the-florida-bar-news/board-of-governors-adopts-ethics-guidelines-for-generative-ai-use/ [https://perma.cc/KE84-7U2P].

41. THE ABA CYBERSECURITY HANDBOOK, *supra* note 4, at 3.

But doing nothing and maintaining the status quo is no longer a viable option for the legal profession. By shifting away from an approach focused only on breach prevention and individual-lawyer decisions to one centered instead on the regulation of lawyer behavior and community-based harm mitigation, the legal profession could better respond to today's data security challenges in ways that are more effective for clients, easier to execute for lawyers, and more enforceable by state bars.

I. THE EVOLVING DUTY OF CLIENT CONFIDENTIALITY: FROM SECRECY TO SECURITY

It is difficult to overstate the longstanding centrality of confidentiality to the lawyer-client relationship. Its many descriptions include: "a vital element in the lawyer's professional function,"[42] "a well-established feature of the American legal system,"[43] one of "the oldest of the privileges" known to the common law,[44] "deeply entrenched,"[45] "the pivotal element of the modern American lawyer's professional functions,"[46] a requirement "the sanctity of [which] seemed beyond question,"[47] "the most ancient and revered of the evidentiary protections cognizable at common law,"[48] and the "bedrock principle of legal ethics"[49] that "goes back to the reign of Elizabeth [I], where the privilege already appears as unquestioned."[50]

Yet statements like these tend to obscure the significant ways in which the lawyer's duty of confidently has changed over time. In fact, although the underlying purpose of confidentiality "to encourage full and frank communication between attorneys and their clients"[51] has not changed,

---

42. Geoffrey C. Hazard, Jr., *Rules of Legal Ethics: The Drafting Task*, 36 REC. ASS'N BAR N.Y.C. 77, 79 (1981).

43. Elizabeth G. Thornburg, *Sanctifying Secrecy: The Mythology of the Corporate Attorney-Client Privilege*, 69 NOTRE DAME L. REV. 157, 157 (1993).

44. Louise L. Hill, *Emerging Technology and Client Confidentiality: How Changing Technology Brings Ethical Dilemmas*, 16 B.U. J. SCI. & TECH. L. 1, 3 (2010) (quoting 8 JOHN HENRY WIGMORE, EVIDENCE § 2290 (McNaughton Rev. 1961)).

45. Steven Goode, *Identity, Fees, and the Attorney-Client Privilege*, 59 GEO. WASH. L. REV. 307, 313 (1991).

46. Geoffrey C. Hazard, Jr., *An Historical Perspective on the Attorney-Client Privilege*, 66 CAL. L. REV. 1061, 1061 (1978).

47. Robert J. Anello, *Justice Under Attack: The Federal Government's Assault on the Attorney-Client Privilege*, 1 CARDOZO PUB. L. POL'Y & ETHICS J. 1, 1 (2003).

48. Jared S. Sunshine, *Seeking Common Sense for the Common Law of Common Interest in the D.C. Circuit*, 65 CATH. U. L. REV. 833, 833 (2016).

49. Daniel R. Fischel, *Lawyers and Confidentiality*, 65 U. CHI. L. REV. 1, 1 (1998).

50. Hazard, *An Historical Perspective*, *supra* note 46, at 1069.

51. Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

the details of the duty of confidentiality have. These changes have included not only *what* client information lawyers must (or must not) be disclosed and *when* lawyers are permitted (or not) to disclose it, but also *how* lawyers must protect these client confidences. This Part focuses on chronicling this latter, procedural shift from lawyer-client confidentiality as a duty solely focused on data secrecy to one focused equally on data security.

A. Client Confidentiality as Data Secrecy

Despite its long-standing importance, the concept of lawyer-client confidentiality was not always the absolute and all-encompassing duty it is today.[52] In fact, for much of the profession's early history, lawyers had no freestanding duty of confidentiality at all.[53] Rather, in its earliest form, lawyer-client confidentiality was exclusively an evidentiary privilege—and a narrow one at that.[54] In late sixteenth and early seventeenth century English courts, the duty's requirements were, in the words of Professor Geoffrey C. Hazard Jr., "narrowly defined and tenuously established."[55] The privilege "was thought to belong to the lawyer rather than the client," "was applied only with much hesitation," and covered information related only to "communications in furtherance of pending litigation."[56] It took centuries for the privilege to expand in size and scope to belong to the client, not the lawyer, and to protect all lawyer-client communications, including transactional matters and strategic advice as opposed to litigation-based communication alone.[57]

Although in mid-nineteenth century America there was an "organization [and] revival of local bar associations . . . [as well as academic] commentators [that] made attempts at systematic statements of the ethics of the profession, seeking order by prescription,"[58] none of these early statements included a freestanding duty of lawyer-client

52. Hazard, *An Historical Perspective*, *supra* note 46, at 1070 ("Taken as a whole, the historical record is not authority for a broadly stated rule of privilege or confidence.").

53. *Id.*

54. *See* Mitchel L. Winick, Brian Burris & Y. Danaé Bush, *Playing I Spy with Client Confidences: Confidentiality, Privilege and Electronic Communications*, 31 TEX. TECH. L. REV. 1225, 1228–29 (2000); Hazard, *An Historical Perspective*, *supra* note 46, at 1070.

55. Hazard, *An Historical Perspective*, *supra* note 46, at 1073.

56. *Id.* at 1070, 1071, 1076.

57. *See id.* at 1070; Winick et al., *supra* note 54, at 1229 ("A significant change in the attorney-client privilege occurred during the early 1700s when ownership of the privilege shifted from the attorney to the client.").

58. Hazard, *Rules of Legal Ethics*, *supra* note 42, at 80.

confidentiality.[59] Instead, the first national statement of legal ethics promulgated by the ABA in 1908 known as the *Canons of Professional Ethics* "did not include a provision requiring lawyers to protect client confidences" and only referenced confidentiality in passing when discussing the need to prevent conflicts of interest.[60]

Specifically, Canon 6 stated that "the obligation to represent the client with undivided loyalty and not to divulge his secrets or confidences forbids also the subsequent acceptance of retainers or employment from others in matters adversely affecting any interest of the client with respect to which confidence has been reposed."[61] Although it is "possible to read this language as . . . articulating a general rule of confidentiality," there is no evidence that the ABA was "concerned about whether clients needed a blanket promise of confidentiality" at the time of the adoption of the *Canons*.[62] In 1927, Canon 37 was added, which emphasized that the "duty to preserve [a] client's confidences outlasts the lawyer's employment."[63] But it was not until 1937 when the ABA amended Canon 37 that the *Canons* "unequivocally expressed the obligation of a lawyer to preserve a client's confidences,"[64] stating explicitly that "[i]t is the duty of a lawyer to preserve his client's confidences."[65]

The *Canons of Ethics*—including this freestanding duty of client confidentiality—gained widespread adoption by state bars.[66] But, in 1964, ABA President Lewis Powell, Jr. proposed creating the Special Committee on Evaluation Standards as a first step to crafting a new set of professional responsibility standards to replace the *Canons*.[67] Five years later, the ABA adopted the *Code of Professional Responsibility*—the successor to the *Canons*.[68] Like the version of the *Canons* that

---

59. *See* Lloyd B. Snyder, *Is Attorney-Client Confidentiality Necessary?*, 15 GEO. J. LEGAL ETHICS 477, 485–86 (2002).

60. *Id.* at 486; *see also* Michael S. Ariens, *"Playing Chicken": An Instant History of the Battle over Exceptions to Client Confidentiality*, 33 J. LEGAL PROF. 239, 243 (2008). The 1908 *Canons* were based in large part on the 1887 Alabama State Bar's comprehensive *Code of Ethics* which focused primarily on "honor and consciences" as well as "calls for [better] professional behavior." *See* MICHAEL S. ARIENS, THE LAWYER'S CONSCIENCE: A HISTORY OF AMERICAN LAWYER ETHICS 114 (2023). Although there was no rule on confidentiality, an oath to "maintain the confidence and preserve inviolate the secrets of . . . client[s]," was included along with the adoption of the *Canons*. Ariens, "*Playing Chicken*," *supra* at 243.

61. CANONS OF PROF. ETHICS Canon 6 (AM. BAR ASS'N 1908).

62. Snyder, *supra* note 59, at 486–87.

63. *Id.* at 487.

64. *Id.* at 487–88.

65. *Id.*

66. *See* ARIENS, THE LAWYER'S CONSCIENCE, *supra* note 60, at 127.

67. *Id.* at 199.

68. *Id.* at 202; Snyder, *supra* note 59, at 490.

immediately preceded it, the *Code of Professional Responsibility* included an express duty of confidentiality.[69] Specifically, DR 4-101 stated that "a lawyer shall not knowingly . . . reveal a confidence of a client" absent a client's statement demonstrating "the intention of [his] client to commit a crime . . . ."[70] This "expanded version" of confidentiality that focused explicitly on preventing "knowing disclosure" made sense for its time.[71] After all, the risk of unauthorized or accidental disclosure was small when client confidences were stored either in lawyers' brains or individual offices.

But given the rapidly shifting nature of law practice, the *Code* did not last long.[72] Less than a decade later, the ABA once again set out to refine the duties of professional conduct for lawyers. This time, the objective was to craft rules that were not merely aspirational but more closely resembled a mandatory standard of minimum conduct—a "law of lawyers" that could be enforced with remedies including, but not limited to, disbarment.[73] The Kutak Commission led this new effort that included "lawyers in practice, judges, legal scholars, persons with extensive experience in government legal services, and lay persons" from "geographically diverse" areas.[74] After many rounds of edits and debate, the ABA House of Delegates adopted the Kutak Commission's proposal in 1983 as the *Model Rules of Professional Conduct*. Like the *Canons* and the *Code* that preceded it, the *Model Rules* contained a robust, freestanding, and "if possible, even more expansive" duty of confidentiality.[75] In its final form, Model Rule 1.6(a) stated that "[a] lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent" or "disclosures [are] impliedly authorized in order to carry out the representation."[76]

Although the *Model Rules* neither expressly used the word "knowingly" nor the phrase "a lawyer shall not reveal," the non-binding comments that accompanied the rule made clear that the focus of the duty remained the prevention of "knowing" and "intentional" disclosure. This secrecy-focused rule of client confidentiality was eventually adopted by

---

69. MODEL CODE OF PRO. RESP. DR 4-101 (AM. BAR ASS'N 1969).

70. *Id.*

71. *See* Snyder, *supra* note 59, at 490.

72. *See* ARIENS, THE LAWYER'S CONSCIENCE, *supra* note 60, at 208 (quoting former ABA President David R. Brink's statement that "[t]he practice of law changed more in the [1970s] than in the entire preceding century.").

73. *Id.* at 207–08.

74. Hazard, *Rules of Legal Ethics*, *supra* note 42, at 77.

75. Snyder, *supra* note 59, at 491.

76. MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 2012).

every state bar and, with minimal alterations, remains operative in every jurisdiction in the United States to this day.[77]

B. The Duty of Confidentiality in the Age of Consumer Technology

Despite the ABA's best efforts, it did not take long for the secrecy-focused duty of confidentiality adopted in the 1983 *Model Rules of Professional Conduct* to become outdated. Specifically, in terms of confidentiality, although the fear of *knowing* and *affirmative* disclosure remained, by the late 1980s and early 1990s the increased use of consumer technology like personal computers, the internet, and e-mail introduced new and unforeseen concerns primarily relating to fears of *accidental* or *unauthorized* disclosure of and access to client confidences.[78]

The challenge was that traditional forms of lawyer-client communication—in-person meetings, letters, phone calls, and even faxes—were not "easily intercepted."[79] By contrast, unencrypted e-mail's digital transmission and storage created unprecedented opportunities for unknowing disclosure resulting from accidents (like sending an e-mail to the wrong recipient) and from unauthorized technological access by third parties (like hackers).[80] The profession, therefore, faced a new question implicated by an old duty: should lawyers be permitted to communicate with clients using unencrypted e-mail despite the confidentiality risks?[81]

Early answers to this question favored forbidding the use of unencrypted e-mail by lawyers. In 1986, the ABA published a special report concluding that "an attorney *should not* communicate confidential matters over an electronic network without first being assured of the reliability of the system in maintaining confidential communications 'either through bar approval or the lawyer's own informed evaluation.'"[82] The two earliest state bars to confront the issue took a similar position by cautioning against lawyers' use of unencrypted e-mail given the confidentiality risks.[83] Their reasoning was simple: unencrypted e-mail was less secure than other means of communication like phone and fax

77. *See infra* Appendix A.

78. ABA Comm. on Ethics & Pro. Resp., Formal Op. 99-413 (1999) (considering whether the use of unencrypted e-mail by lawyers violates Model Rule 1.6(a)).

79. Winick et al., *supra* note 54, at 1240.

80. *Id.* at 1244 ("Unlike traditional mail, when an attorney sends an electronic message the original message is not actually 'sent'.").

81. *See* Formal Op. 99-413.

82. Winick et al., *supra* note 54, at 1249 (citing ABA Comm. on Lawyers' Resp. for Client Protection, *Lawyers on Line: Ethical Perspectives in the Use of Telecomputer Communication* (1986) at 67 (emphasis added)).

83. *See* Iowa Bar Ass'n Ethics Op. 97-01 (1997); N.C. State Bar Ops. RPC 215 (1995).

and, as a result, lawyers should be required to either get client consent in advance or at least determine whether or not using unencrypted e-mail was appropriate given the specific risk profile of the client and data at issue.[84]

That said, this restrictive approach to using e-mail did not last long. Every subsequent state bar that considered the question concluded—rightly or wrongly—that it was permissible to use unencrypted e-mail to communicate confidential client information was permissible in the absence of unusual circumstances.[85] These opinions typically reasoned that e-mail technology was not inherently more risky than other types of digital communications.[86] They also typically relied on the *Electronic Communications Privacy Act of 1986* which defined the privacy expectations of e-mail users.[87] Under this reasoning, just as lawyers enjoyed a reasonable expectation of privacy in using phone lines, mail, and fax, they enjoyed a reasonable expectation of privacy in e-mail as well.

In 1999, the ABA adopted this new, majority approach. The Standing Committee on Ethics and Professional Responsibility addressed the issue of unencrypted e-mail in Formal Opinion 99-413 titled "Protecting the Confidentiality of Unencrypted E-Mail."[88] In this Formal Opinion, after explaining the unique confidentiality challenges faced by lawyers wishing to communicate via unencrypted e-mail, the Committee concluded that "[l]awyers have a reasonable expectation of privacy in communications made by all forms of e-mail" such that "a lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the internet without violating the *Model Rules of Professional Conduct*."[89]

The justification in Formal Opinion 99-413 was similar to the state bars that had already reached similar conclusions. Specifically, the Committee wrote that "[t]he same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail."[90] It continued that "[t]he risk of unauthorized interception and disclosure

84. Winick et al., *supra* note 54, at 1252.

85. *Id.* at 1253.

86. *Id.*

87. *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 99-413, at 2 n.2 (1999) (citing that statute as a justification for the conclusion that "[i]t is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law.")

88. Formal Op. 99-413.

89. *Id.*

90. *Id.*

exists in every medium of communication, including e-mail."[91] But, it continued, "[i]t is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law."[92] The Formal Opinion did, however, identify an important exception to this otherwise categorical rule. If "the lawyer reasonably believes that confidential client information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted," it explained, "the lawyer should consult the client as to whether another mode of transmission, such as special messenger delivery, is warranted."[93]

Yet, in practice—and perhaps not entirely surprisingly—lawyers focused less on the default rule that e-mail communication was permitted and more on identifying the "special circumstances" where it could not be used.[94] Although the Formal Opinion specifically envisioned situations where unencrypted e-mail might not be permissible, Formal Opinion 99-413 failed to provide any meaningful guidance about how to make that assessment.[95]

This, once again, led to the ABA clarifying the duty of confidentiality. Along with other professional duties called into question by the new adoption of consumer technology, the ABA formed the "Ethics 2000 Commission" to produce a comprehensive reevaluation of the *Model Rules of Professional Conduct* given "new issues and questions raised by the influence that technological developments are having on the delivery of legal services,"[96] including the issues of confidentiality raised by e-mail. The Committee recommended—and in 2002 the ABA House of Delegates approved—the adoption of two new, non-binding comments to Model Rule 1.6(a) to guide lawyers about how to maintain this "duty of confidentiality."[97]

New comment 15 to Model Rule 1.6 explained that lawyers needed to "safeguard information relating to the representation of a client

91. *Id.*

92. *Id.*

93. *Id.*

94. *Id.*

95. *Id.* (at most requiring lawyers to "consult the client").

96. E. Norman Veasey, Chair of ABA Comm'n on Evaluation of Rules of Pro. Conduct, Chair's Introduction (Aug. 2002), https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_preface/ethics_2000_chair_introduction/.

97. *See* MODEL RULES OF PRO. CONDUCT r. 1.6 cmts 15, 16 (AM. BAR ASS'N, Draft 2000), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/e2k_migated/10_85rem.pdf

against . . . inadvertent or unauthorized disclosure."[98] New comment 16, building on Formal Opinion 99-413, stated that "the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients . . . [but] does not require the lawyer to use special security measures if the method of communication affords a reasonable expectation of privacy."[99] This comment also emphasized that "[s]pecial circumstances . . . may warrant special precautions" and identified several "factors to be considered in determining th[eir] reasonableness" including (1) the "sensitivity of the information" and (2) "the extent to which the privacy of the communication is protected by law or by a confidentiality agreement."[100]

C. Client Confidentiality as a Duty of Data Security

Although important steps, neither Formal Opinion 99-413 nor the addition of comments 15 and 16 to Model Rule 1.6(a) provided sufficient guidance to lawyers about applying the duty of confidentiality to the increasingly technological practice of law. In 2009, the ABA formed yet another commission to update the *Model Rules of Professional Conduct* to "keep pace with societal change" given the "accelerating pace of technological innovation" such as "the proliferation of personal computing, e-mail, 'smart-phone' technology, enhanced personal digital assistants, and the internet."[101] This Commission, referred to as the Ethics 20/20 Commission, was chaired by two prominent attorneys: Jamie Gorelick, a former United States Deputy Attorney General, and General Counsel to the Department of Defense, and Michael Traynor, a former President of the American Law Institute. The duty of confidentiality was one key area on which the Commission focused its efforts.[102]

After an extensive process,[103] the Commission recommended, and the ABA House of Delegates adopted, the addition of new subsection (c) to Model Rule 1.6. Specifically, this subsection elevated the language

98. *Id.*

99. *Id.*

100. *Id.* cmt 16.

101. *See* JAMIE S. GORELICK & MICHAEL TRAYNOR, ABA COMMISSION ON ETHICS 20/20, ABA COMMISSION ON ETHICS 20/20 PRELIMINARY ISSUES OUTLINE (2009), https://www.bankruptcylitigation.blog/wp-content/uploads/sites/427/uploads/file/outline-1.pdf [https://perma.cc/2VYD-3JT6]; ARIENS, THE LAWYER'S CONSCIENCE, *supra* note 60, at 279.

102. *See* ARIENS, THE LAWYER'S CONSCIENCE, *supra* note 60, at 279 (explaining that "the result was both stasis and modest change . . . [where] most amendments reflected changes in how attorney-client communications were protected including information storage and delivery").

103. *See ABA Commission on Ethics 20/20: Outreach*, AM. BAR ASS'N, https://www.americanbar.org/groups/professional_responsibility/committees_commissions/aba-commission-on--ethics-20-20/outreach/ [https://perma.cc/V9TU-7CGT].

previously contained in the non-binding comments to the text of Model Rule 1.6. New subsection (c) required, for the first time, "a lawyer to make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[104]

This seemingly simple, twenty-six-word requirement was at once a natural progression of the lawyer's duty of confidentiality and at the same time a paradigm shift in the centuries-old lawyer-client relationship. Although the Commission explained that "this duty [wa]s already described in several existing Comments . . . in light of the pervasive use of technology to store and transmit confidential client information" it was necessary to take "the existing obligation" and state it in the "black letter" of the *Model Rules*.[105] The Commission offered three specific justifications for this change: (1) an increase in inadvertent disclosure "such as when an e-mail . . . is sent to the wrong person"; (2) the greater regularity of third party "'hacks' into a law firm's network or a lawyer's e-mail account"; and (3) the reality that "employees or other personnel [can more easily] release [confidential information] without authority."[106]

In addition the Commission recommended, and the ABA adopted, two additional, non-binding comments to clarify how lawyers were supposed to execute this new duty of data security. New comment 15 (now comment 18) identified a set of non-exclusive factors that a lawyer must consider when taking "reasonable efforts" to prevent unauthorized or inadvertent disclosure. These factors included assessing:

(1) "the sensitivity of the information,"
(2) "the likelihood of disclosure if additional safeguards are not employed,"
(3) "the cost of employing additional safeguards, the difficulty of implementing the safeguards," and
(4) "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)."[107]

Comment 16 (now comment 19) added to those factors that "[t]his duty . . . does not require that the lawyer use special security measures if

104. MODEL RULES OF PROF. CONDUCT r. 1.6, (AM. BAR ASS'N 2012).

105. *See* AM. BAR ASS'N COMM. ON ETHICS 20/20, REPORT TO THE HOUSE OF DELEGATES 2, 4 (2012), https://nysba.org/NYSBA/Content%20Conversion/Round%201/Content%20Folder/ExcludefromSearch/20072008Coursebooks/_2012COURSEBOOKS/_2012COURSEBOOKSAssets/Topic-4-Commission-on-Ethics.pdf [https://perma.cc/RL3J-JUNC].

106. *Id.* at 4.

107. MODEL RULES OF PROF. CONDUCT r. 1.6 at cmt 15. (AM. BAR ASS'N 2012) (now comment 18).

the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions."[108] Specific transmission factors to be considered include: (1) "the sensitivity of the information," and (2) "the extent to which the privacy of the communication is protected by law or by a confidentiality agreement."[109]

Ultimately, the addition of Model Rule 1.6(c) and its comments not only elevated the previously aspirational duty of data security to a binding part of the lawyer's duty of confidentiality, but it also identified several touchstones for implementing that duty going forward. First, it emphasized that the central focus of the duty of data security was preventing unauthorized and accidental access as well as disclosure by using the correct technological safeguards. Second, it made clear that this duty belonged to the individual lawyer taking custody of individual client confidences. Third, unlike Formal Opinion 99-413 that preceded it, this approach refused to offer categorical rules about the specific technologies that lawyers could or could not use. Instead, it required individual lawyers to balance the sensitivity of specific client information on the one hand against the cost, difficulty, and availability of other technological safeguards on the other. Fourth, it adopted a reasonableness approach as opposed to one based on strict liability.

Together, these touchstones implicated the adoption of a new set of lawyer competencies and considerations. It presumed, for example, that lawyers understood the confidential information acquired from their clients and had the technical ability and knowledge to identify and select from the various technological safeguards that they could employ. In this way, this duty of data security was tied to comment 6 (now comment 8) to Model Rule 1.1's duty of competence which requires technological competence as part of a lawyer's general duty of competence.[110] This comment, which was also adopted as part of the Ethics 20/20 Commission's recommendations, requires lawyers to "keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology."[111]

Although individual state bars were not required to adopt the approach, thirty-one states have adopted Model Rule 1.6(c) and some version of the new comments verbatim.[112] Nine states and the District of Columbia chose not to adopt Rule 1.6(c) but did adopt comments instructing lawyers

108. *Id.*

109. MODEL RULES OF PROF. CONDUCT r. 1.6 cmt. 17. (AM. BAR ASS'N 2012) (now comment 19).

110. MODEL RULES OF PROF. CONDUCT r. 1.1 cmt. 6 (AM. BAR ASS'N 2012) (now comment 8).

111. *Id.*

112. *See infra* Appx. A for a detailed summary of which states have adopted Model Rule 1.6(c).

to take reasonable precautions to safeguard confidential information just like Model Rule 1.6(c) requires.[113] Four states have adopted Rule 1.6(c) but have omitted the comments (although in some instances, like in Louisiana, that is simply because their state rules of professional conduct do not have any comments).[114] Six states chose not to adopt Rule 1.6(c) or its comments but have instead published Ethics Opinions on the subject that closely track the *Model Rules of Professional Conduct*.[115] For example, the relevant California Ethics Opinion explains that "[a]n attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology . . . does not subject confidential client information to an undue risk of unauthorized disclosure."[116] As a result, all fifty state bars and the District of Columbia Bar have adopted the ABA's approach to the duty of data security in some form.

Yet lawyers have continued to look for greater guidance on what they can, should, and must do in order to protect client confidences. In 2017, the ABA issued a non-binding Formal Opinion focused on providing greater clarity on this topic.[117] In a Formal Opinion titled "Securing Communication of Protected Client Information" the Standing Committee on Ethics and Professional Responsibility explained that although the ABA had "updat[ed] the Comments to Rule 1.1 . . . and add[ed] paragraph (c) . . . to Rule 1.6" in the five years since its adoption "the term 'cybersecurity' has come into existence."[118] Although it is certainly not the case that the term "cybersecurity" was new,[119] this Formal Opinion correctly recognized that the Model Rule 1.6(c) did not give a great deal of concrete guidance. The Committee wrote, in a "post-Opinion 99-413 world where law enforcement discusses hacking and data loss in terms of 'when,' and not 'if,'" it was necessary to "discuss factors other than the *Model Rules of Professional Conduct* that lawyers should consider when using electronic means to communicate regarding client matters."[120] Whether these factors are equivalent to those outlined in comments 18 and 19 or are simply aspirational and separate is not entirely clear from the text of the Opinion. That said, lawyers that wish to follow all relevant

113. *Id.*

114. *Id.*

115. *Id.*

116. Cal. State Bar Comm. on Pro. Resp. and Conduct, Formal Op. 2010-179 (2010).

117. *Id.*

118. ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017).

119. *See* Jeff Kosseff, *Defining Cybersecurity Law*, 103 IOWA L. REV. 985, 986 (2018) (discussing the federal Cybersecurity Act of 2015).

120. Formal Op. 477R.

ABA guidance on the topic must now balance the four non-exclusive factors listed in comments 18 and 19 to Model Rule 1.6 as well as the seven additional factors laid out in Formal Opinion 477R.[121] These factors include:

(1) understanding the nature of the threat;
(2) understanding how client confidential information is transmitted and where it is stored;
(3) understanding and using reasonable electronic security measures;
(4) determining how electronic communications about client matters should be protected;
(5) labeling client confidential information;
(6) training lawyers and non-lawyer assistant in technology and information security and
(7) conducting due diligence on vendors providing communication technology.[122]

In addition to these seven specific considerations, the ABA issued additional Formal Opinions that touch on data security and confidentiality duties, including Formal Opinion 480 (on blogging) and Formal Opinion 483 (on duties following a data breach). The ABA also published a *Cybersecurity Handbook* that spans 720 pages and costs more than $100, even for current ABA members, which contains other suggestions and cybersecurity best practices.[123]

The transition from an evidentiary privilege focused on secrecy to a freestanding duty of data security is an important but underdiscussed shift in the legal duty of confidentiality. But despite the near universal adoption of the ABA's approach, the duty of data security unfortunately remains anything but clear given the various binding and non-binding factors that individual lawyers must weigh on a confidence-by-confidence basis. More than that, as the next Part will show, the current approach to this duty has proven far less successful than the ABA had hoped.

II. CHALLENGES WITH THE CURRENT APPROACH TO THE LAWYER'S DUTY OF DATA SECURITY

The prior Part explored how the duty of data security became an integral part of the contemporary lawyer's broader duty of confidentiality.[124] It also described the reality that it has been adopted

121. *Id.*
122. *Id.*
123. THE ABA CYBERSECURITY HANDBOOK, *supra* note 4.
124. *See supra* Part I.

nearly universally by state bars.[125] Unfortunately, this widespread adoption does not mean that the approach proved successful. To the contrary, as scholars and practitioners have noted, and this Part further explores, there are a number of significant shortcomings with this current approach.[126]

In an attempt both to explain why a new approach to the lawyer's duty of data security is necessary and what that approach should look like, this Part catalogs three of the most significant shortcomings with the current approach to that duty. First, it explains why the duty is not *effective* at fulfilling its stated purpose of preventing unauthorized and accidental access and disclosure of confidential client information. Second, it explores why the duty is difficult, if not impossible, to *execute* by everyday lawyers. Third, it describes the ways that this duty has been difficult, if not impossible, to *enforce* by state bars—and why this failure of enforcement is problematic for the legal profession.

A. Effectiveness Problems

Journalists called 2023 a "banner year" for data breaches in the legal profession.[127] Prominent law firms like Kirkland & Ellis, K&L Gates, and Proskauer Rose all suffered public data breaches by the ransomware group Clop.[128] Another prominent law firm, Covington & Burling, was subpoenaed by the SEC for information related to a prior data breach that may have compromised client data.[129] Hackers even breached the ABA—the entity responsible for promulgating the professional rules of conduct

125. *See supra* Part I.

126. *See, e.g.*, Wald, *supra* note 6, at 518 ("Rule 1.6(c) and Comments 18 and 19 fall short in several respects."); Natasha Babazadeh, *Legal Ethics and Cybersecurity: Managing Client Confidentiality in the Digital Age*, 7 J.L. & CYBER WARFARE 85, 109 (2018) ("The rules of professional responsibility in the United States and abroad must be reformed to consider cybersecurity and the role that technology plays in the legal profession."); Pardau & Edwards, *supra* note 2, at 71 ("Sixteen different state bar associations have made various attempts to help attorneys navigate the issue of cloud computing, but their opinions on cloud computing are generally impractical and blind to the attorney's lack of leverage with vendors."); Myles G. Taylor, *Seeing Clearly? Interpreting Model Rule 1.6(c) for Attorney Use of Cloud Computing Technology*, 45 MCGEORGE L. REV. 835, 837 (2014) ("[W]hile the rule's current iteration succeeds as a general rule clarifying the existence of an affirmative safeguard obligation, it fails to provide real instruction and guidance to attorneys in practice who are seeking to meet their ethical obligations.").

127. Nelson et al., *supra* note 5.

128. *Id.*

129. *Id.*

related to confidentiality—putting the private information of its more than 1.5 million attorney members at risk.[130]

Despite headlines like these, data breaches in the legal profession are not a new phenomenon. In 2022, commentators wrote that leaks and disclosures "soared" in the legal profession.[131] During that year, the profession witnessed notable incidents such as Alex Jones' e-discovery case where a lawyer accidentally shared *all* of Mr. Jones's text messages and then failed to properly claw them back before trial,[132] the accidental disclosure of e-mails about the January 6th insurrection when counsel failed to deactivate a Dropbox link,[133] and the unauthorized leak of the draft of the United States Supreme Court's decision in the *Dobbs v. Jackson Women's Health Organization* case.[134] In 2021, several law firms, including Jones Day and Goodwin Proctor, suffered a major data breach when Accellion, a third party data transfer company, was hacked[135] and the New York City Law Department suffered a data breach that limited remote access to case materials for months resulting in numerous case postponements.[136] In 2020, the law firm of Grubman Shire Meiselas & Sacks was forced to pay more than $300,000 after hackers leaked information related to Lady Gaga and other celebrity clients.[137] In 2019, the lawyers for Paul Manafort, President Trump's former campaign manager, failed to properly redact PDF documents[138] and it was reported that "more than 100 law firms" suffered data breaches.[139] In 2018, hackers

---

130. Sara Merken, *ABA Says Hackers Took Lawyers' Data in March Attack*, REUTERS (Apr. 21, 2023), https://www.reuters.com/legal/litigation/aba-says-hackers-took-lawyers-data-march-attack-2023-04-21/ (last visited Sept. 16, 2024).

131. Marathe, *supra* note 39.

132. Collins, *supra* note 4.

133. Marathe, *supra* note 39.

134. *Id.*

135. Chris Opfer, *Jones Day Hit by Data Breach as Vendor Accellion Hack Widens*, BLOOMBERG LAW (Feb. 16, 2021), https://news.bloomberglaw.com/business-and-practice/jones-day-hit-by-data-breach-as-vendor-accellion-hacks-widen [https://perma.cc/WBB5-E8RL].

136. Katie Honan, *New York City Law Department Hit by Cyberattack*, WALL ST. J. (June 7, 2021, 8:13 PM), https://www.wsj.com/articles/new-york-city-law-department-hit-by-cyberattack-11623105336 (last visited Sept. 16, 2024).

137. *Biggest Legal Industry Cyber Attacks*, ARCTIC WOLF (Apr. 30, 2024), https://arcticwolf.com/resources/blog/top-legal-industry-cyber-attacks [https://perma.cc/UHM5-RFBV].

138. Louis Matsakis, *Paul Manafort Is Terrible with Technology*, WIRED (Jan. 9, 2019), https://www.wired.com/story/paul-manafort-bad-tech-pdfs-passwords/ [https://perma.cc/4VQU-YKW2].

139. Christine Simmons, Xiumei Dong & Ben Hancock, *More Than 100 Law Firms Have Reported Data Breaches. And the Problem Is Getting Worse*, BLOOMBERG LAW (Oct. 15, 2019), https://www.law.com/international-edition/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse-378-123883/ [https://perma.cc/BUQ5-CY62].

on the dark web tried to sell entire law firm networks for as little as $3,500.[140] In 2017, the law firm of DLA Piper was "hit by a major cyber attack" that "knocked out phones and computers across the firm" worldwide for days resulting in millions of dollars in costs.[141] And in 2016, the Panamanian law firm Mossack Fonseca suffered one of the largest and most impactful data breaches of all time when a self-described "whistleblower" confiscated and disclosed 2.6 terabytes of client data from the firm's e-mail servers related to the activities of offshore shell companies used by prominent world figures dating back to 1970.[142]

This is just a small sample of the publicly reported data breaches and data security failures by lawyers, law firms, and legal associations over the past decade. Many other data security failures by lawyers have been reported and one can only imagine the size and scope of the breaches and disclosures that never came into public view.

The aggregate statistics are even more disturbing. According to recent studies, as many as 80% of big law firms report being targeted by hackers,[143] as many as one in four lawyers report suffering a "security breach,"[144] and as many as one in forty data breaches worldwide occur in the legal or insurance industries.[145] As a result, in the words of Professor Daniel Solove, "law firms are facing grave privacy and security risks . . . . On a scale of 1 to 10, the risks law firms are facing are an 11."[146]

Although the adoption of Model Rule 1.6(c) and the ABA's subsequent guidance likely prevented some number of additional data breaches, the sheer scale of data security failures by lawyers and the legal profession

---

140. Jennifer Schlesinger & Andrea Day, *Hackers Are Selling Access to Law Firm Secrets on Dark Web Sites*, CNBC (July 12, 2018, 12:09 PM), https://www.cnbc.com/2018/07/11/hackers-selling-access-to-law-firm-networks-on-dark-web-sites.html [https://perma.cc/45SA-AMDJ].

141. James Booth, *DLA Piper Hit by Cyber Attack with Phones and Computers down Across the Firm*, ALM (June 27, 2017), https://www.law.com/international-edition/2019/10/15/more-than-100-law-firms-have-reported-data-breaches-and-the-picture-is-getting-worse-378-123883/ [https://perma.cc/9Z96-PP8U].

142. THE ABA CYBERSECURITY HANDBOOK, *supra* note 4, at 25–27 (detailing the scale of the Panama Papers breach); Will Fitzgibbon, *Panama Papers FAQ: All You Need to Know About The 2016 Investigation*, INT'L CONSORTIUM INVESTIGATIVE JOURNALISM (Aug. 21, 2019), https://www.icij.org/investigations/panama-papers/panama-papers-faq-all-you-need-to-know-about-the-2016-investigation/ [https://perma.cc/5PWE-2QBB].

143. Debra Cassens Weiss, *Representing clients in China? Prepare to be hacked; BigLaw is a frequent target*, AM. BAR ASS'N J. (Mar. 11, 2015), https://www.abajournal.com/news/article/representing_clients_in_china_prepare_to_be_hacked_biglaw_is_a_frequent_tar [https://perma.cc/64VR-JN78].

144. Simek, *supra* note 20.

145. Skolnik et al., *supra* note 19.

146. Daniel J. Solove, *Law Firm Cyber Security and Privacy Risks*, LINKEDIN (Apr. 23, 2015), https://www.linkedin.com/pulse/law-firm-cyber-security-privacy-risks-daniel-solove/ [https://perma.cc/6QT9-ACWK].

indicates that, at the very least, the current approach to the duty of data security is not as effective as it could be. More than that, though, what these data security failures demonstrate is how little the current approach to this duty in the *Model Rules* responds to the most common client confidentiality failures that lawyers and legal associations face.

For example, one of the most common ways that hackers breach law firms and legal organizations is through phishing scams and ransomware.[147] These scams typically start with an e-mail that looks legitimate but is designed to mislead an individual recipient into either sharing their login credentials directly or clicking on a link that downloads a file that grants the attacker access to a lawyer's network.[148] Once the hacker gains access, they threaten to shut down the network, delete files, or reveal client confidences or other private information unless the law firm or legal association pays them a large sum of money.[149] Even if these efforts are caught before confidential client information is transferred, they often force the firm or organization to shut down legitimate access to their networks in order to preserve the integrity of the data and investigate.[150] Whether or not the ultimate disclosure occurs, the breach creates significant costs when attorneys—who are often paid on the billable hour—are unable to conduct business. It is no secret in the legal profession that many lawyers, law firms, and legal organizations have suffered ransomware and phishing attacks.[151] "Smishing" adds another similar security threat, where SMS text messaging is used to infiltrate employer networks from well-meaning employees.[152] And the dangers

147. THE ABA CYBERSECURITY HANDBOOK, *supra* note 4, at 27–28 ("Ransomware . . . is a massive cyber threat for organizations . . . such as law firms."); Cai Thomas, *The Phishing Techniques Law Firms Are Falling For*, INFO. AGE (June 20, 2019), https://www.information-age.com/phishing-techniques-law-firms-14036/ [https://perma.cc/TZ3P-MRJY] (noting that "[p]hishing is now the most common cyber attack affecting the legal sector" and that "80% of law firms reported phishing attempts").

148. *See Phishing Scams*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams [https://perma.cc/X893-UMCF]; *How to Recognize and Avoid Phishing* Scams, FED. TRADE COMM'N, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams [https://perma.cc/5JKT-BXLZ].

149. *See Ransomware Hits Law Firms Hard-And It's Worse Than Ever Before*, LOGIKCULL, https://www.logikcull.com/blog/maze-ransomware-law-firms [https://perma.cc/F262-AGA3].

150. *See* Joe Patrice, *Cybersecurity Incident Shuts Down Biglaw Network*, ABOVE THE L. (Feb. 9, 2023, 11:43 AM), https://abovethelaw.com/2023/02/cybersecurity-incident-shuts-down-biglaw-network/ [https://perma.cc/G72F-WZZP].

151. Simmons et al., *supra* note 139; THE ABA CYBERSECURITY HANDBOOK, *supra* note 4, at 28 ("Lawyers and law firms . . . have been targeted . . . [and t]he threat continues to grow more serious.").

152. *See* Jim Calloway & Ivan Hemmans, *The 411 on Texting for Lawyers*, N.C. BAR ASS'N, 11 (2018), https://www.ncbar.org/wp-content/uploads/2019/04/The-411-on-Texting-For-Lawyers-OBA-Version.pdf [https://perma.cc/6F9X-EPFT].

can only increase with AI deepfakes, voice cloning, and other modern infiltration tools.

The DLA Piper hack is a good example.[153] There, a single, non-lawyer administrator in the Vault 100 firm's Ukraine office was tricked into downloading a document that contained malware known as NotPetya.[154] Given that the firm had a "flat network structure globally,"[155] this malware quickly spread throughout the firm's worldwide network in minutes disabling the telephone system and most of its computer network for almost a week.[156] "DLA Piper paid over 15,000 hours of overtime to its IT department" and they eventually had to restart their network at a cost to the firm of tens of millions of dollars.[157] Tellingly, though, this disruption was not the result of the type of conduct that Model Rule 1.6(c) seeks to regulate. That is, this was not the result of an unreasonable technological choice by an individual lawyer about the specific technology necessary to protect a specific client confidence. Rather, the harm was caused by a broad attack of an entire law firm's network by a nefarious third party, not by targeting a single lawyer or single client's confidences.

Similarly, "one worker's pilfered email password" led to a disruption to the more than 1,000 lawyers in the New York Law Department.[158] As the *New York Times* noted, the Law Department had failed to implement multifactor authentication two years after the city required it.[159] Although this could have helped avoid the breach, the department-wide choice to allow the entire network to be accessed and compromised by a single set of stolen e-mail credentials ultimately caused the harm from this hack.[160]

These are just two examples of phishing and ransomware attacks on lawyers among many. What these incidents—and so many more like them—illustrate is that the current approach to the duty of data security is not well targeted at preventing and responding to one of the profession's

153. *See* Crozier, *supra* note 141.

154. Jim Carroll, *Do Not Fall Down the Rabbit Hole of a Law Firm Data Breach*, BIGGER L. FIRM, https://www.biggerlawfirm.com/do-not-fall-down-the-rabbit-hole-of-a-law-firm-data-breach/ [https://perma.cc/TWA5-WYJP].

155. Crozier, *supra* note 141.

156. Carroll, *supra* note 154 ("The firm the size of DLA Piper without having access to email for one week is unimaginable.").

157. *Id.*

158. Ashley Southall, Benjamin Weiser & Dana Rubinstein, *This Agency's Computers Hold Secrets. Hackers Got in with One Password.*, N.Y. TIMES (July 9, 2021), https://www.nytimes.com/2021/06/18/nyregion/nyc-law-department-hack.html (last visited Sept. 16, 2024).

159. *Id.*

160. *Id.*

greatest data security risks. The current approach is primarily focused on how individual lawyers can prevent breaches of individual client data over which they take custody. Although this lawyer-by-lawyer, secret-by-secret approach might have made sense in the context of data *secrecy*—after all, only the lawyer who learned of a client secret could affirmatively share it—the ransomware scenario illustrates how this approach makes little sense in the context of data *security*, which often occurs at the law firm or legal association level.

A second common data security challenge faced by lawyers that the Model Rule 1.6(c) prevention-based approach largely leaves unaddressed is accidental disclosures. A high-profile example occurred during the much-publicized defamation trial of right-wing provocateur Alex Jones, introduced above. In that case, Sandy Hook Elementary School parents sued Jones for defamation arising out of false comments made about the shooting.[161] Jones's attorney collected all of Jones's text messages during the relevant period.[162] He then intentionally shared a Dropbox folder containing documents responsive to the plaintiffs' discovery requests but unintentionally shared "the entire contents of [Jones's] phone" along with it.[163] Then, after opposing counsel alerted Jones's counsel to this mistake, he failed to properly claw back the documents pursuant to a procedure provided for in the Texas rules.[164]

Even if the failure to claw back was itself unreasonable, it is hard to understand how the mere collection of client text messages, or the accidental disclosure of those text messages, violates the duty of data security as currently framed by the *Model Rules*. After all, the technology used was exactly the technology used for an effective transfer of discovery seemingly permitted by the rules. The mistake here was human: sharing more than one folder when the lawyer intended to only share one. And this is only one potential lawyer mistake among many similar ones that occur regularly, such as mistyping an e-mail address, dragging-and-dropping the wrong file, or failing to properly set a date-and-time limitation on a shared drive. In short, although technological safeguards can help the situations in which these mistakes can occur, human mistakes will happen. As a result, an approach that focuses solely on technological

161. Collins, *supra* note 4.

162. *Id.*

163. *Id.*

164. *See id.* Notably, Alex Jones' lawyers were sanctioned in Connecticut for mishandling discovery. That said, the decision sanctioning these lawyers focused on the unauthorized transfer of documents acquired by the opposing party subject to a court-entered protective order. The decision did not discuss Rule 1.6. *See* Memorandum of Decision Re Order to Show Cause Attorney Norman Pattis Juris #408681, 2023 WL 153608 (Conn. Super. Ct. Jan. 5, 2023) (order dismissing attorney Norman Pattis).

safeguards that prevent disclosure simply cannot be the only or best way to protect client confidential information.

Most of all, though, even when third parties breach client confidences because of failures in technological safeguards, the current approach to the duty of confidentiality paints technology as the only but-for cause. Take the Panama Papers incident for example. As the *ABA Cybersecurity Handbook* explains, "[t]he Mossack Fonseca breach that compromised the confidential records of the entire firm *was the result* of the failure to provide appropriate data security."[165] But was that the only failure? To be sure, Mossack Fonseca's breach resulted from the firm's failure to update open-source web software that had known security vulnerabilities.[166] But that was certainly not the only reason why the breach caused so much harm. In addition to this technological failure, there was a human failure as well. That failure was the firmwide decision to maintain 2.6 terabytes of highly sensitive confidential information dating back to 1970.[167] That choice contributed just as much to harm to the firm's clients as the failure to patch a security vulnerability in the firm's website software.

Ultimately, lawyers are being targeted for the client confidences they keep. Even when they are not targeted, accidental disclosures inevitably take place. As a result, even if the current approach to the duty of data security embodied in Model Rule 1.6(c), its comments, and its commentaries has had some positive effect, it is beyond time to consider what, if anything, can be done to better address these challenges.

B. Execution Problems

In addition to the effectiveness problems described above, the lawyer's duty of data security suffers from a second set of challenges related to the ability of even the most well-intentioned lawyers to faithfully execute this duty. As this section explores, the duty of data security embodied in Model Rule 1.6(c) rests on three fundamental but faulty assumptions. First, the current duty of data security incorrectly assumes that lawyers have sufficient technical knowledge to understand, assess, and then select from available technological safeguards to prevent unauthorized and accidental access and disclosure. Second, it incorrectly assumes that lawyers have sufficient knowledge of the sensitivity of their client's data and the overall risk (and cost) tolerances of those clients. Third, it incorrectly assumes that lawyers are able, in practice, to balance these two

165. THE ABA CYBERSECURITY HANDBOOK, *supra* note 4, at 27 (emphasis added).

166. *Id.* at 7.

167. *Id.* at 26.

sets of information effectively and efficiently on a confidence-by-confidence basis. This section discusses each in turn.

1. Lawyers Are Not Technological Experts

The current approach to the duty of data security starts from the idea that lawyers have a meaningful level of technological expertise. After all, the text of Model Rule 1.6(c) and its comments make clear that the lawyer's duty of data security is predicated on individual lawyers making "reasonable" choices about what technological "safeguards" to "employ[]" and "implement" in order to "prevent" unauthorized and accidental access and disclosure.[168]

But in reality, lawyers rarely have the technical knowledge, skills, and experience necessary to make these difficult decisions.[169] To be clear, this is not a general critique that lawyers are inherently bad at technology—although there is likely some truth to that claim.[170] Regardless of lawyers' capacity to obtain the required technical expertise, the profession simply does not require maintaining a sufficient level of technological expertise to make "reasonable choices" about appropriate technological safeguards to prevent unauthorized and accidental access of confidential client information. Nor does it sufficiently teach or test those skills in law school or on licensure exams.[171]

To be sure, the ABA likes to highlight that Rule 1.6(c) is predicated in part on the lawyer's duty of technological competence articulated in

---

168. MODEL RULES OF PRO. CONDUCT r. 1.6(c) (AM. BAR ASS'N 2012).

169. *See, e.g.*, John Bandler, *Attorneys on Alert for Cybersecurity Threats: New York's New CLE Training Requirement*, REUTERS (July 19, 2023, 8:42 AM), https://www.reuters.com/legal/legalindustry/attorneys-alert-cybersecurity-threats-new-yorks-new-cle-training-requirement-2023-07-19/ (last visited Sept. 16, 2024) ("Cybersecurity and cybercrime prevention are now solidly part of traditional attorney duties even though universal knowledge and compliance is not yet here.").

170. *See* Heidi Frostestad Kuehl, *Technologically Competent: Ethical Practice for 21st Century Lawyering*, 10 CASE W. RRSV. J.L. TECH. & INTERNET 1, 5 (2019); Jordan Rothman, *Some Lawyers Are Unacceptably Bad with Technology*, ABOVE THE L. (Apr. 1, 2022), https://abovethelaw.com/2022/04/some-lawyers-are-unacceptably-bad-with-technology/ [https://perma.cc/D8SS-82PX]; Patrice, *When Luddites Handle Cyber Security*, *supra* note 7.

171. That is not to say that *some* law schools do not offer cybersecurity curricula. In fact, in August 2023, the ABA's Cybersecurity Legal Task Force not only highlighted the existence of these types of curricula at some law schools but also encouraged that the ABA adopt a resolution urging law schools to "incorporate cybersecurity and emerging technologies into their curricula." *See* Maureen Kelly & Claudia Rast, *Resol. 610: Cybersecurity and Emerging Technologies Curricula in Law Schools*, AM. BAR ASS'N, 1 (Aug. 2023), https://www.americanbar.org/content/dam/aba/directories/policy/annual-2023/610-annual-2023.pdf [https://perma.cc/E5EB-SETZ]. The ABA House of Delegates adopted this Resolution at its August 2023 Annual Meeting. *See id.*

comment 8 to Model Rule 1.1 which was adopted alongside it.[172] This comment requires lawyers to "keep abreast of . . . the benefits and risks associated with relevant technology" as part of their minimum duties of competence.[173] But, even on its face, there is a significant disconnect between the level of technical knowledge required by the text of comment 8 and the level of technical knowledge necessary to faithfully execute Model Rule 1.6(c). "Keep[ing] abreast of . . . the benefits and risks with technology"—even if it were mandatory and not merely included in the non-binding comments to Rule 1.1—is very different from understanding how those underlying technologies work at a level that would allow lawyers to assess the ability of different technological safeguards to effectively prevent data breaches. After all, there is a substantial difference between knowing the benefits and general risks of communicating with e-mail and understanding e-mail encryption technologies, the differences between e-mail service providers' terms of use, and the considerations necessary to select between specific cloud-based or locally stored e-mail service providers.

More than that, neither law school curricula nor licensure exams systematically cover or test these specific skills.[174] Lawyers are not specifically tested on their ability to select among relevant technological safeguards on the mandatory Multistate Professional Responsibility Exam (MPRE) or the Uniform Bar Exam (UBE).[175] Nor is technological training of this kind typically required as part of state bar continuing legal education requirements. One notable exception is the New York State Bar Association which announced in 2022, to great fanfare, that it was adding a cybersecurity training requirement—the first of its kind nationwide.[176] The problem? This requirement can be met by taking any number of courses on any number of cybersecurity-related topics *for a total of one*

---

172. *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017) ("At the intersection of a lawyer's competence obligation to keep 'abreast of knowledge of the benefits and risks associated with relevant technology,' and confidentiality obligation to make 'reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,' lawyers must exercise reasonable efforts when using technology in communicating about client matters.").

173. MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2021).

174. *See* Kelly & Rast, *supra* note 171.

175. *See, e.g.*, *Preparing for the MPRE*, NAT'L CONF. OF BAR EXAMINERS, https://www.ncbex.org/exams/mpre/preparing-mpre [https://perma.cc/WZW7-M6LL] (explaining that the MPRE "is based on the law governing the conduct and discipline of lawyers and judges," but not identifying the application of Rule 1.6(c) as an area of focus); *Preparing for the MBE*, NAT'L CONF. OF BAR EXAMINERS, https://www.ncbex.org/exams/mbe/preparing-mbe [https://perma.cc/CHZ6-QTEL] (identifying the "seven subject areas: Civil Procedure, Constitutional Law, Contracts, Criminal Law and Procedure, Evidence, Real Property, and Torts.").

176. Bandler, *supra* note 169.

hour every two years.[177] This is far from a robust commitment to giving lawyers the technological skills necessary to engage in the kind of technology-specific decision-making envisioned by the Model Rule 1.6(c) approach.[178]

Of course, these CLE-type requirements could be expanded, and some individual lawyers can, and do, gain this knowledge on their own.[179] Individual law firms and legal organizations may require lawyers to undergo additional technology and data security training either at the direction of management or because they are mandated to by clients or insurers.[180] But these additional training opportunities are "extras," not requirements of fulfilling a lawyer's duty of confidentiality. That they are not required to fulfill a lawyer's duty of minimum competence calls into question whether Model Rule 1.6(c)'s vision for data security, which is based primarily, if not exclusively, on the selection of reasonable technological safeguards, calls for a set of skills that minimally competent lawyers simply do not have.[181]

From a data security perspective, predicating the lawyer's duty on a base level of knowledge that most lawyers do not have is, at best, problematic and, at worst, dangerous. After all, some lawyers who are aware of their ignorance on technical topics will simply select the path of least resistance (or least cost)—which is often doing nothing at all—especially given the complete lack of enforcement discussed in greater depth below.[182] Others who wish to faithfully execute these duties will take on greater financial and time burdens to learn what they believe they need to know.[183] Still, others who are unconsciously incompetent of their

177. *Cybersecurity Privacy and Data Protection FAQs*, N.Y. STATE UNIFIED CT. SYS., https://www.nycourts.gov/LegacyPDFS/attorneys/cle/Cybersecurity-Privacy-and-Data-Protection-FAQs.pdf [https://perma.cc/XVX5-QAMJ].

178. *See id.*

179. Although as scholars have recognized, CLE requirements are likely not an effective way to accomplish the goal of increased competence generally. *See* Rima Sirota, *Making CLE Voluntary and Pro Bono Mandatory: A Law Faculty Test Case*, 78 LA. L. REV., 547, 548 (2017).

180. *Cybersecurity for Law Firms: What Legal Professionals Should Know*, AM. BAR ASS'N (Dec. 29, 2022), https://www.americanbar.org/groups/law_practice/resources/tech-report/2022/cybersecurity-law-firms/ [https://perma.cc/V4LT-8M7Y] ("The firm's cyberinsurance carrier will likely require cybersecurity awareness training for employees.").

181. *See* Kuehl, *supra* note 170, at 13 ("After adopting cloud computing services, attorneys need to also understand how to use those services with the mammoth amount of client confidential information that might be stored therein and also must safeguard client files by using enhanced security measures or reasonably protect data in the cloud.").

182. *See infra* section II.C.

183. *See* Leonard Wills, *How to Become a Cybersecurity Lawyer*, AM. BAR ASS'N (Nov. 2, 2018), https://www.americanbar.org/groups/litigation/resources/newsletters/minority-trial/how-become-cybersecurity-lawyer/ (last visited Sept. 18, 2024).

technical knowledge will make what they believe to be informed data security decisions based on what they *think* is more secure, even if those decisions cost more and protect less.[184]

It comes down to this: Model Rule 1.6(c)'s approach creates a duty based in no small part on the technical knowledge of individual attorneys. Although some lawyers will have this technological knowledge, and others can afford to hire technological experts to support them, a rule that requires as its foundation that lawyers have a specific level of technical expertise but fails to require or even provide the tools necessary to develop that expertise, rests on a faulty and dangerous foundation.

2. Lawyers Do Not Have Sufficient Knowledge About Client Risks and Risk Tolerances

Even assuming that lawyers have the technical expertise necessary to make "reasonable" decisions about the proper technological "safeguards" to implement, they often do not have sufficient knowledge of the "sensitivity of the information" that they take from their clients as Model Rule 1.6(c) requires, nor are they required to learn their clients' cost and risk preferences related to that data.[185]

On the first challenge—having insufficient knowledge of client data—there are a number of structural problems in contemporary legal practice. First, there is almost always a delay between when lawyers learn what client data they hold and when the risks for unauthorized or accidental access or disclosure of that data begin. This happens because lawyers often take digital custody of client data before they review it. After all, it is not uncommon for clients to share digital data with lawyers either by e-mail or through shared digital hard drives or cloud storage programs. Yet the risk of unauthorized access or disclosure of that data begins the moment that the lawyer takes custody of that data even though, by definition, the lawyer has not had a chance to review it or assess how sensitive the data is. It makes little sense to predicate a risk assessment on knowledge about the specific level of sensitivity of client data when lawyers do not know the sensitivity of that data when the disclosure risk begins.

Second, this also assumes—often incorrectly—that lawyers will eventually review the confidential client data they receive. In contemporary legal practice, clients regularly turn over large quantities of

---

184. *See Poor Decision-Making Can Lead to Cybersecurity Breaches*, MSUTODAY (Feb. 14, 2015), https://msutoday.msu.edu/news/2015/poor-decision-making-can-lead-to-cybersecurity-breaches [https://perma.cc/NLZ8-QAVH].

185. MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 2021).

digital data to their lawyers for their review with full knowledge that the lawyer will not ultimately review every document. Instead, lawyers in many different areas of practice—litigation, transactional, and regulatory—regularly review only a subset of the client information that they take based on keywords, date limiters, or document types. As United States District Court Judge Tanya Chutkan recently explained during a high-profile discovery dispute, "[d]iscovery in 2023 is not sitting in a warehouse with boxes of paper looking at every single page."[186]

Lawyers are at an even further disadvantage when it comes to assessing the "sensitivity" component of the Model Rule 1.6(c) for one additional reason: the rule permits—but does not require—clients to participate in discussions about how lawyers protect against the disclosure of client confidences.[187] Unlike in many other Model Rules (including Model Rule 1.6(a)), comment 18 to Model Rule 1.6(c) states 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."[188] Some scholars have suggested that, in addition to Model Rule 1.6(c), Model Rule 1.4 separately requires lawyers to communicate with clients "about the means by which the client's objectives are to be accomplished," which includes security-related decisions about client confidentiality.[189] But, at best, the requirement to coordinate with clients is uncertain.[190] As a result, the current approach permits an information asymmetry where clients, who are often in a better position than their lawyers to assess data security costs and benefits, need not be and are not consulted when making data security decisions. This is a mistake.

3. Lawyers Are Unable to Effectively and Efficiently Balance Technological Safeguards Against Client Risks

Finally, assuming that lawyers have sufficient technical knowledge and sufficient knowledge about client data and client risk tolerances, lawyers are also required to use this knowledge to engage in a complex and constant balancing process to select adequate technological safeguards on a confidence-by-confidence basis. The *Model Rules of Professional*

186. Ryan J. Reilly, *Federal Judge Sets Trump Trial Date in Election Interference Case*, NBC NEWS (Aug. 28, 2023, 1:42 PM), https://www.nbcnews.com/politics/donald-trump/federal-judge-set-trump-trial-date-election-interference-case-rcna101669 [https://perma.cc/6UP3-79PE].

187. MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18.

188. *Id.* (emphasis added).

189. *See* Drew T. Simshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data*, 38 AM. J. TRIAL. ADVOC. 549, 560 (2015).

190. *See id.*

Conduct make this clear when they emphasize in the comments that a lawyer must assess "the sensitivity of the information" as part of the reasonableness inquiry.[191] Given that different confidences for the same client might be more or less sensitive, the rule seems to imply a confidence-by-confidence assessment.

But this also makes little sense given the contemporary practice of law. In the United States today, the average "civil case typically contains around 130 gigabytes, or 6.5 million pages of data, gathered from 10 to 15 custodians—roughly equivalent to the number of pages you would need to fill 100 pickup trucks."[192] As a result, unlike prior generations when a confidence-by-confidence assessment was perhaps possible, the digital transfer from client to lawyer of massive amounts of data makes such a confidence-by-confidence basis is at best impracticable.

On top of the quantity of confidences, the factor-based assessment is made even more challenging by the sheer quantity of factors that the current approach encourages, if not requires, a lawyer to consider. Even if a lawyer focused *only* on Model Rule 1.6(c), the comments to that rule, and Formal Opinion 477R, they would need to consider *eleven different factors* when making data security decisions. And in some states, which include additional factors in Ethics Opinions, the number of factors that a lawyer is required to consider swells to as many as thirty.[193] In short, even with the right information, requiring lawyers to engage in a confidence-by-confidence assessment of reasonable technological safeguards makes little sense.

C. Enforcement Problems

Finally, in addition to effectiveness and execution challenges, the current approach to the duty of data security faces another significant but underdiscussed hurdle, which is that the duty of data security has proven completely unenforceable in practice. In fact, although Model Rule 1.6(c) has been on the books for more than a decade (and its requirements were a part of the comments to Model Rule 1.6(a) for more than a decade before that), there is not a single published disciplinary action for violating this duty of data security in the digital context.[194]

---

191. MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18.

192. *eDiscovery Opportunity Costs: What Is the Most Efficient Approach?*, LOGIKCULL, https://www.logikcull.com/blog/ediscovery-opportunity-costs-infographic [https://perma.cc/S5QU-7X4P].

193. Pardau & Edwards, *supra* note 2, at 78–79.

194. This conclusion is not easy to confirm. Records of disciplinary actions for forty-nine of fifty states and the District of Columbia are searchable to varying degrees online. For some states, it was

Of course, the mere existence of a duty can affect lawyer behavior. Rules of professional conduct serve as a kind of deterrent for lawyers[195] and are used in malpractice cases as probative evidence of the relevant standard of care.[196] Yet, having a duty of data security but not enforcing that duty *at all* should cause us to question the benefits of the approach. To be sure, there are several potential explanations for this wholesale lack of enforcement. One might be that the "reasonableness" approach simply makes it too hard to enforce—a challenge we have seen in similar reasonableness-based data security standards enforced by the FTC.[197] In that context, some federal courts of appeal have called into question the enforceability of reasonableness standards, which do not sufficiently provide advance guidance on the data security efforts that must be taken.[198] If this is the primary challenge, a more concrete, easier-to-apply rule might permit greater state-bar enforcement. For example, state bars regularly enforce Model Rule of Professional Conduct 1.15's requirement that lawyers may not comingle client funds—and lawyers are regularly sanctioned for violating this duty.

Another potential explanation is that clients are rarely made aware of these breaches.[199] When they are, they seek to find recourse in other ways that can better remedy their harm rather than going after their lawyers' ability to practice.[200] A third potential explanation is simply that many of

---

possible to review each disciplinary action to identify a violation of Rule 1.6(c) on file. For others, natural language searching was used for keywords such as "data breach," "data leak," and "confidentiality." Finally, for those state bar websites with no search or sorting function a manual review of selections of disciplinary actions from the records of each state going back at least ten years was conducted. Despite all of these different approaches to finding a relevant disciplinary action, no such actions were found.

195. *See Premable & Scope* of MODEL RULES OF PRO. CONDUCT, ¶ 16 (AM. BAR ASS'N 2021) ("Compliance with the Rules, as with all law in an open society, depends primarily upon understanding and voluntary compliance, secondarily upon reinforcement by peer and public opinion and finally, when necessary, upon enforcement through disciplinary proceedings.").

196. *See* McKee, *supra* note 30, § 2 ("Although it is generally recognized that the intent of professional ethical codes is to establish a disciplinary remedy rather than to create civil liability, many courts have determined that pertinent ethical standards are admissible as evidence relevant to the standard of care in legal malpractice actions . . . .").

197. William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1138–39 (2019).

198. *See* LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1236 (11th Cir. 2018).

199. Wald, *supra* note 6, at 535 ("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.").

200. *See What if I Am Unhappy With My Lawyer?*, AM. BAR ASS'N (Jun. 7, 2018), https://www.americanbar.org/groups/public_education/resources/public-information/what-if-i-am-unhappy-with-my-lawyer-/ ("Be aware that making a complaint of this sort may punish the lawyer for misconduct, but it will probably not help you recover any money.").

these breaches fail to create sufficient "harm" to the clients. [201] The harm is often borne instead by the lawyers who need to shut down digital access while security vulnerabilities are assessed and patched.[202] A fourth potential explanation is just a general discomfort by the bar with enforcing a duty that substantially relies on technological sophistication that it knows most lawyers do not have.

No matter the reason, this lack of enforceability by state bars is problematic. Even if unenforced rules have some deterrent effect, a *complete* lack of enforcement creates two problems. First, a complete lack of enforcement diminishes the deterrent effect.[203] Lawyers who see other lawyers suffer public breaches—either by hack or by accident—but who suffer no public consequences are less likely to engage in the costly and time-consuming process of making "better" data security decisions to avoid similar situations in the future.

Second, and perhaps even more fundamental, this lack of enforcement lessens the rule's effect because it fails to allow for the profession to build a common law around what constitutes reasonable behaviors in specific circumstances. Without published decisions helping to define reasonable efforts in particular practice areas, it remains challenging, if not impossible, for the concept of reasonableness to be further defined and clarified for future cases. This is where the analogy to other reasonableness tests found in the law begin to fall flat. Although lawyers are certainly familiar with and generally supportive of reasonableness standards, rarely do they exist in a judicial-decision vacuum.

The reality that no state bar has enforced Model Rule 1.6(c) in more than a decade since its adoption undermines the foundational principles on which it is based. Although the duty of data security needs to be flexible enough for different types of legal practice and constantly emerging technologies, it must also be concrete enough to permit enforcement. A rule that is not enforceable (or executable or effective, for that matter) simply does not sufficiently serve lawyers or their clients.

---

201. *See You Can Sue Your Law Firm Over Data Breach, but Good Luck Winning*, LOGIKCULL, https://www.logikcull.com/blog/can-sue-law-firm-data-breach-good-luck-winning [https://perma.cc/H6HT-DSGR].

202. *See, e.g.*, Crozier, *supra* note 141 (highlighting the significant costs of locking down a law firm's digital security after a breach).

203. *See* Fred C. Zacharias, *What Lawyers Do When Nobody's Watching: Legal Advertising as a Case Study of the Impact of Underenforced Professional Rules*, 87 IOWA L. REV. 971, 997 (2002) ("A fair reading of the breadth of the codes suggests that the drafters never intended full enforcement. Many provisions are designed primarily to offer guidance to lawyers."); Daniel S. Nagin, *Deterrence in the Twenty-First Century*, 42 CRIME & JUST. 199, 201 (2013) ("I conclude, as have many prior reviews of deterrence research, that evidence in support of the deterrent effect of various measures of the certainty of punishment is far more convincing and consistent than for the severity of punishment.").

That is why the legal profession requires a new approach to its duty of data security.

III. A NEW APPROACH TO THE LAWYER'S DUTY OF DATA SECURITY

Part I of this Article discussed how and why the duty of data security became a central part of the lawyer's longstanding duty of confidentiality.[204] Part II then described the significant shortcomings with the current approach to that duty despite its widespread adoption by state bars.[205] With this history and these challenges as its backdrop, this Part now offers a normative proposal for how to improve the lawyer's duty of data security going forward in ways that both honor the duty's history and purpose but also respond to the serious theoretical and practical shortcomings with the current approach described above.

A. From Breach Prevention to Harm Mitigation

The defining characteristic of the current approach to the lawyer's duty of data security is its focus on the technological security measures that individual lawyers must take to prevent data security breaches. The text of Model Rule 1.6(c) makes this clear when it defines "reasonable efforts" as those which "*prevent* inadvertent or unauthorized disclosure of, or unauthorized access to," client confidences.[206] The comments then take this one step further by defining reasonable efforts in this context as requiring individual lawyers to balance "the sensitivity" of specific client confidences against "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."[207] Analogizing to the protection of client confidences in the physical world, this approach is like a requirement that lawyers select the proper type of lock to put on the door to the room where client confidences are stored.

On its face, this approach makes some intuitive sense. After all, if lawyers take "reasonable efforts" to prevent unauthorized and accidental access and disclosure, one might presume that fewer such incidents will take place. And, the logic continues, if fewer incidents take place because technological safeguards prevent them, then the confidentiality harms to

204. *See supra* Part I.

205. *See supra* Part II.

206. MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 2021) (emphasis added).

207. *Id.* at cmt 18.

clients from unauthorized access and disclosure will be lessened, if not eliminated.

Unfortunately, this could not be further from the truth. As Professor Scott J. Shapiro explained in a *New York Times* Op-Ed titled *This Is Why I Teach My Law Students How to Hack*:

> If cybercrime is a sophisticated high-tech feat, we assume, the solution must be too. Cybersecurity companies hype proprietary tools like "next generation" firewalls, anti-malware software and intrusion-detection systems. Policy experts like John Ratcliffe, a former director of national intelligence, urge us to invest public resources in a hugely expensive "cyber Manhattan Project" that will supercharge our digital capabilities.
>
> But this whole concept is misguided. The principles of computer science dictate that there are hard, inherent limits to how much technology can help. Yes, it can make hacking harder, but it cannot possibly, even in theory, stop it. What's more, the history of hacking shows that the vulnerabilities hackers exploit are as often human as technical — not only the cognitive quirks discovered by behavioral economists but also old-fashioned vices like greed and sloth.[208]

Put another way, as Professors Solove & Hartzog explain in their influential 2022 book *Breached!: Why Data Security Law Fails and How to Improve It*, "we can't eliminate all breaches, but we can significantly reduce the harm that they cause."[209]

Although there is no single set of agreed-upon data security "best practices" today, most private and public data security frameworks look beyond technological safeguards and breach prevention. The Center for Internet Security (CIS), for example, focuses on the "processes and technical controls to identify, classify, securely handle, retain, and dispose of data."[210] The National Institute of Standards and Technology (NIST) identifies five "core functions" that not only include preventing breaches technologically, but also the processes and people necessary to "govern, identify, protect, detect, respond, and recover" data.[211] The Federal Trade Commission's "Start with Security: A Guide for Business" recommends

---

208. Scott J. Shapiro, Opinion, *This Is Why I Teach My Law Students How to Hack*, N.Y. TIMES (May 23, 2023), https://www.nytimes.com/2023/05/23/opinion/cybersecurity-hacking.html (last visited Sept. 16, 2024).

209. SOLOVE & HARTZOG, *supra* note 35, at 13.

210. *CIS Critical Security Control 3: Data Protection*, CTR. FOR INTERNET SEC., https://www.cisecurity.org/controls/data-protection/ [https://perma.cc/2KLU-Y3ED].

211. *See The CSF 1.1 Five Functions*, NAT'L INST. STANDARDS & TECH.: CYBERSECURITY FRAMEWORK (Feb. 26, 2024), https://www.nist.gov/cyberframework/online-learning/five-functions [https://perma.cc/V35Q-PPPU].

ten different data security best practices of which only three relate to technological breach prevention.[212] And the European Union's General Data Protection Regulation (GDPR) focuses on "people [and] process" in addition to technology.[213]

This is for good reason. Although most data security frameworks include "architectural requirements" to prevent unauthorized access, they also all include "systems of compliance" to prevent harm from access as well.[214] These systems of compliance regulate "human decisionmaking and process" because "[i]t has long been a platitude in IT management that technological safeguards are only one component of data security."[215] The "best data security frameworks," as Professor William McGeveran explains, focus on the "golden triangle" that includes technology but also people and processes.[216]

Unfortunately, for the past two decades, the legal profession's approach to the duty of data security has focused primarily on the technology leg of this triangle. This myopic focus on individual lawyers' decisions about the technological safeguards necessary to prevent breaches is not only its defining feature but is also its greatest bug. In fact, many of the challenges discussed in Part II can be traced directly back to this singular focus on technological breach prevention. This focus requires lawyers to (1) be technical experts in areas that are beyond their training and expertise, (2) know the sensitivity of client data and client risk tolerances when they rarely do and, (3) make difficult, if not impossible, individualized assessments of client confidences. It makes the lawyer's duty of data security difficult if not impossible to enforce and it has proven largely unsuccessful at guiding lawyers or protecting clients in a world where data breaches are a matter of when, not if.

One possible response to this challenge is to adopt a rule that explicitly outlines the precise technological breach prevention measures that lawyers must adopt rather than relying on a fact-specific, reasonableness

---

212. *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Aug. 2023), https://www.ftc.gov/system/files/ftc_gov/pdf/920a_start_with_security_en_aug2023_508_final_0.pdf [https://perma.cc/DWF7-SK7R].

213. *Six Lessons We've Learned About the GDPR*, CIO (Mar. 7, 2018), https://www.cio.com/article/228502/six-lessons-we-ve-learned-about-the-gdpr.html [https://perma.cc/H4FA-V8VC] ("If there was a program that required focus on people, process, and technology, GDPR is it.").

214. McGeveran, *supra* note 197, at 1180, 1188.

215. *Id.* at 1181; *see also* Justin Hurwitz, *Response to McGeveran's the Duty of Data Security: Not the Objective Duty He Wants, Maybe the Subjective Duty We Need*, 103 MINN. L. REV. HEADNOTES 139, 141–42 (2019) ("[S]ecurity is about process, not state . . . . [such that] good security . . . is not about achieving a state of being secure, but is about approaching security as on ongoing activity.").

216. McGeveran, *supra* note 197, at 1181.

approach. Several commentators have indicated their support for just that approach.[217] For example, Professor Eli Wald argues that one critical way to improve Model Rule 1.6(c) and its comments would be to "defin[e] 'reasonable efforts'" to include minimum, specific "basic cybersecurity measures" that all lawyers must follow including, for example, a requirement to use "virus scanners," "firewalls," and "cryptographically strong passwords."[218]

There are certainly benefits to the adoption of a set of minimum technological standards for lawyers. At the very least, this approach would clarify what lawyers must do to discharge their duty of confidentiality and would "put lawyers on notice" of requirements that could serve as a "framework to penalize lawyers for any violations."[219] That said, while the adoption of a more explicit set of technological safeguards would certainly provide more clarity,[220] abandoning or minimizing the reasonableness approach to the lawyer's duty of data security would leave many of the other concerns discussed above unaddressed and present some new challenges as well.

As a threshold matter, adopting this approach risks turning the lawyer's duty of data security into a "'check-a-box' procedure for purposes of avoiding discipline" that might come to be treated as a kind of "safe harbor."[221] That is, lawyers might believe that if they adopt the specific minimum technological standards expressly laid out in the rule, they have complied with their duty. But checklist approaches to data security often do more harm than good[222] and are generally disfavored by data security experts for several reasons.[223]

First, checklist data security standards quickly end up being under-protective because "the inevitability of rapid technological change [is such that b]oth threats and solutions evolve too quickly to keep precise rules up to date."[224] Unless the ABA and state bars regularly update these

---

217. Wald, *supra* note 6, at 527; Babazadeh, *supra* note 126; Ellen Platt, Comment, *Zooming into a Malpractice Suit: Updating the Model Rules of Professional Conduct in Response to Socially Distanced Lawyering*, 53 TEX. TECH L. REV. 809, 811 (2021).

218. Wald, *supra* note 6, at 529.

219. Babazadeh, *supra* note 126, at 110; *see also* Platt, *supra* note 217, at 839 ("Primarily, it would provide a starting point for attorneys who find little to no interpretive guidance under Comment [18].").

220. *See supra* sections II.B, II.C.

221. Wald, *supra* note 6, at 530.

222. SOLOVE & HARTZOG, *supra* note 35, at 196.

223. *See, e.g.*, *id.* at 49 ("The standards approach is only used in a handful of security laws."); McGeveran, *supra* note 197, at 1199 ("Those who seem to crave a rule for data security instead of a standard should be careful what they wish for.").

224. McGeveran, *supra* note 197, at 1198.

minimum standards—something they have not proven particularly effective at—they have the potential to become out of date as soon as they are adopted.[225] Reasonableness-based approaches, on the other hand, maintain the flexibility necessary to handle constantly evolving technologies as opposed to creating a never ending game of cat and mouse.[226]

Second, minimum-standard approaches have the potential to be overprotective as well. Even if some explicit, technological data security requirements are generally useful in some or even most cases, they are rarely necessary for every case—and requiring too much in data security systems can be as problematic as requiring too little. Technological safeguards always create costs—time, convenience, and monetary expense—and those costs are real and affect lawyer and client behaviors. Perhaps counterintuitively, the imposition of confidentiality costs when the risks do not outweigh the benefits tends to make the underlying confidential data less secure.[227] As Professors Solove and Hartzog explain, "[i]t is easy to underappreciate the costs of many security measures . . . the biggest costs of many security measures are that they can reduce functionality, make things inefficient and inconvenient, and be difficult and time consuming."[228] "Counterintuitively," they continue, "if security measures are *too* protective, they might lead to bad security outcomes because people create workarounds and other dangerous kludges that bypass protective systems entirely or weaken them."[229]

In the context of the legal profession, requiring all lawyers to adopt a specific technological solution—such as encryption—has been regularly rejected for just these reasons. As the Standing Committee put it in Formal Opinion 477R, "[w]hat constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors . . . [which] depend on the multitude of possible types of information . . . the methods of electronic communications employed, and the types of available security measures for each method."[230] In other words, even if requiring encryption would prevent some data security

225. For example, the Ethics 20/20 Commission recommended that the "Center for Professional Responsibility coordinate with other ABA entities to establish centralized and up-to-date websites to help lawyers address critical and constantly evolving ethical . . . issues related to technology and outsourcing." ABA COMMISSION ON ETHICS 20/20, INTRODUCTION & OVERVIEW 2 (2012). Tellingly, no such website was created. The idea is not inherently a bad one. It is, however, an idea that simply does not fit with the ABA's traditional approach to regulating lawyer conduct.

226. McGeveran, *supra* note 197, at 1198.

227. SOLOVE & HARTZOG, *supra* note 35, at 11.

228. *Id.*

229. *Id.* at 182–83.

230. ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017).

breaches today, the costs of imposing mandatory encryption for all lawyers in all contexts is simply too great.

Third, even if a set of minimum data security standards is adopted as a "floor [but not a ceiling] for appropriate cyber conduct,"[231] as some suggest, lawyers will then be required to incur all of the costs associated with these minimum-security measures but still be left with insufficient clarity about how to discharge their duty. That is essentially what happened when the ABA adopted Formal Opinion 99-413, discussed above.[232] There, the ABA tried to create a categorical rule permitting the use of unencrypted e-mail while leaving an exception for "special circumstances."[233] The problem was that lawyers were then focused almost exclusively on what constituted "special circumstances," leaving lawyers (and their clients) unable to rely on the general rule. Similarly, here, adopting minimum standards that are sufficient in most but not all cases leaves the same burden on attorneys but would drastically increase the costs. More than that, these costs would largely be borne by small firms and solo practitioners who cannot afford to hire technical specialists and face a greater personal risk of failing to undertake "reasonable efforts."

Fourth, even if a set of explicit minimum-security standards might prove easier to execute for lawyers, that does not mean that being more explicit will be more effective at protecting client confidences. In fact, many of the data security failures by lawyers discussed above occurred despite effective technological safeguard decisions, not because of ineffective ones. This too should come as no surprise. As Solove & Hartzog remind us, "[d]ata security . . . is not really a war between technologies that attack and technologies that protect. Instead, data security is a struggle with people using technologies"[234] and "[a]t its core, data security is about humans."[235] Therefore, even if a technology-specific minimum standard might be an improvement in some ways, it is neither the only nor the best way to reform the duty of data security for lawyers going forward.

Another potential response to the rule's shortcomings described above would be to simply remove lawyers from executing the duty of data security altogether. This is essentially the argument advanced by practitioners Stuart L. Pardau & Blake Edwards in their thought-

231. Wald, *supra* note 6, at 530.

232. *See supra* section I.B.

233. *Id.*

234. SOLOVE & HARTZOG, *supra* note 35, at 71.

235. *Id.*

provoking article *The Ethical Implications of Cloud Computing*.[236] There, they argue that the *Model Rules of Professional Conduct* should simply require lawyers to use non-lawyers to respond to inevitable data security challenges.[237] Specifically, their approach would require lawyers to get (1) "informed consent" from their clients about data security decisions, (2) use "specialty cloud providers" to make digital security choices, and (3) carry "cyber insurance" to cover the costs of a breach should it occur.[238] But this approach simply swings too far in the opposite direction. After all, even if it correctly presumes that data security breaches will inevitably occur, it incorrectly presumes that lawyers are therefore unable to play a meaningful role in protecting client confidences.[239] There is a reason that, despite the existence of cybersecurity experts and cyber insurance, modern data security frameworks do not simply require holders of confidential or private information to outsource data security decision-making and risks onto third parties. As the discussion below elaborates, lawyers need to be a part of the solution to data security challenges, even if they cannot solve the problem alone.

The remainder of this Part therefore proposes another approach. It argues that the legal profession can and should maintain a robust, reasonableness-based duty of data security, but that it should reframe the focus of that reasonableness inquiry. Specifically, rather than regulating technological breach prevention measures, it argues that the rules should focus on regulating *how* lawyers interact with digital client confidences and *who* lawyers are required to coordinate with when making data security decisions.

Textually, this shift could be accomplished quite simply. In fact, it would require the addition of only two words to the rule itself.[240] Instead of mandating that lawyers take "reasonable efforts to prevent inadvertent or unauthorized disclosure of, or unauthorized access" to client data, the approach would require lawyers to take "reasonable efforts to prevent *harm from* inadvertent or unauthorized disclosure of, or unauthorized access." Of course, merely adding these two words to Model Rule 1.6(c) is not enough. We cannot simply replace one overly general and difficult to execute rule of confidentiality with another. But by defining this harm-prevention approach through the specific processes that lawyers must engage in and the people with whom lawyers must work when making

236. *See* Pardau & Edwards, *supra* note 2.

237. *See id.*

238. *Id.* at 72.

239. *See infra* sections III.B, C.

240. *Infra* Appx. B.

data security decisions, the profession can integrate all three legs of the "golden triangle" discussed above—technology, process, and people—into the lawyer's duty of data security. Although these shifts alone will not solve all of the challenges facing lawyers in the age of cloud computing, they at least offer a vision for the lawyer's duty of data security that builds on data security best practices and responds to the effectiveness, execution, and enforcement challenges described above.

B. Process

To incorporate harm mitigation into the lawyer's duty of data security, the duty must shift in focus from regulating the technologies that lawyers use and must understand, to regulating the processes and behaviors of lawyers when they interact with client confidences regardless of the technology used. To be sure, this shift will still require lawyers to grapple with the inherent risks of the technologies they use—but only as part of a larger process. This is important because, as many contemporary data security regimes recognize, the harm of data breaches is rarely attributable to a single technological choice made by a single person about a single piece of data at a single moment. Instead, these harms most often result from a large number of decisions and practices while confidential information is held.[241] As a result, regulating the processes and behaviors throughout the data-storage lifecycle has the ability not only to mitigate the *number of* breaches that take place but also the *harm from* breaches.

There are several different ways to operationalize this proposed theoretical shift. Building on contemporary data security frameworks, this section proposes four: (1) a requirement that lawyers consider whether specific client data must be held and for how long ("data minimization"); (2) a requirement that lawyers consider ways to segregate client's data where possible ("data segregation"); (3) a requirement that lawyers track on what systems client data is stored and who has access to those systems ("data mapping"); and (4) a requirement that lawyers maintain client-specific data security plans ("data security planning").[242]

---

241. SOLOVE & HARTZOG, *supra* note 35, at 75 ("Because organizations that suffer breaches are not the only cause of the breaches or the only actors that can affect the risk, the law should facilitate a better management of the risk across the entire data ecosystem."); *id.* at 79 ("Numerous actors play a role in data breaches beyond the organizations that suffer the breach.").

242. Although there are a number of different ways to integrate these specific rules into the Model Rules, the most obvious would be to integrate them into the Comments to Model Rule 1.6(c). Specific proposed language is included in Appendix B below.

1. Data Minimization

"Data Minimization" refers to the practice of requiring individuals collecting private data to "collect only data [that is] necessary for the purpose at hand and to avoid retaining unnecessary data."[243] The benefit of data minimization should be obvious: "[d]ata that doesn't exist can't be compromised" which "soften[s] the impact" when data breaches occur.[244] Unlike requirements that focus on selecting secure technologies, data minimization focuses on the quantity of data collected in the first place and how long that data is held.[245] As a result, data minimization can mitigate harm from data security breaches regardless of the technology used, the technical knowledge of the individual using it, or the but-for cause of the breach. Given how effective data minimization is at mitigating the harmful effects of breaches, it has become a common feature of many contemporary data security regimes such as GDPR,[246] HIPAA, [247] FTC guidance,[248] and privacy by design,[249] just to name a few.[250]

Requiring lawyers to consider data minimization as part of their data security decision-making process would almost certainly have an immediate impact similar to its adoption in other data security frameworks. That said, the idea that the rules of professional conduct for lawyers should encourage lawyers to collect fewer client confidences might seem counterintuitive, if not downright antithetical, to the practice of law. After all, lawyers are well-known for collecting as much client information as possible and holding that information for a long period of

---

243. SOLOVE & HARTZOG, *supra* note 35, at 146.

244. *Id.*

245. *Id.* at 156 ("The idea that companies should only be able to collect and retain data that is adequate, relevant, and necessary is a bulwark against data abuse . . . .").

246. *See* Glossary for Letter "D," EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/glossary/d_en [https://perma.cc/A6WE-WNTF].

247. Office for Civil Rights, *Minimum Necessary Requirement*, U.S. DEP'T HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html [https://perma.cc/5UAP-C439] (referred to in HIPAA as the "minimum necessary requirement").

248. *Start with Security*, *supra* note 212.

249. Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, U.C. SANTA CRUZ, https://privacy.ucsc.edu/resources/privacy-by-design---foundational-principles.pdf [https://perma.cc/PQ2Z-CXQ9].

250. Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2259 (2015) ("Almost all data security regulatory regimes that use a reasonableness standard include . . . [d]ata minimization.").

time, if not indefinitely.[251] In fact, that is one justification for the duty of confidentiality and the attorney-client privilege in the first place. Because lawyers need as much client data as possible in order to provide the best representation possible, the argument goes, the attorney-client privilege and the professional duty of confidentiality are necessary to encourage clients to freely disclose that information.[252] Although Model Rule 1.16(d) requires lawyers to "surrender[] papers and property to which the client is entitled" when a representation ends,[253] lawyers typically hold a significant amount of confidential client information after the end of a representation, both to support the creation of future work product and to protect themselves in the event that they are sued for malpractice.

But while this lawyer-collect-all approach may have made sense in the pre-digital age when the benefit of collecting client confidences was meaningful and the risks of disclosure were minimal, that is simply no longer the case. Any number of high-profile examples illustrate this point, but perhaps none illustrates it better than the Panama Papers case described above.[254] There, roughly 11.5 million documents were leaked dating back to 1970 were disclosed.[255] Although a technology failure was the but-for cause of the breach, the harm from that breach was exacerbated by the firm's decision to store massive amounts of client confidential information that in some cases was more than forty years old.[256] Had the law firm Mossack Fonseca taken less confidential information from their

---

251. *See*, *e.g.*, George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?*, 13 RICH. J.L. & TECH. 1, 10 (2007) ("Perhaps more easily grasped, the amount of information in business has increased by thousands, if not tens of thousands of times in the last few years. In a small business, whereas formerly there was usually one four-drawer file cabinet full of paper records, now there is the equivalent of two thousand four-drawer file cabinets full of such records, all contained in a cubic foot or so in the form of electronically stored information. This is a sea change."); Whitney Morgan, *Baring All: Legal Ethics and Confidentiality of Electronically Stored Information in the Cloud*, 24 CATH. U. J.L. & TECH 469, 484 (2016) ("Most lawyers do not know the first thing about cybersecurity, yet they unknowingly store confidential information in the cloud as a default option on a daily basis.").

252. Fred C. Zacharias, *Rethinking Confidentiality*, 74 IOWA L. REV. 351, 352–53 (1989) ("[C]lients won't confide in lawyers without confidentiality; lawyers need it to represent clients effectively."); Fischel, *supra* note 49, at 26 ("Without confidentiality rules, clients would be less willing to disclose negative information to their attorney[].").

253. MODEL RULES OF PRO. CONDUCT r. 1.16 (AM. BAR ASS'N 2021).

254. Fitzgibbon, *supra* note 142.

255. *Id.*; Will Kenton, *The Panama Papers Scandal: Who Was Exposed & Consequences*, INVESTOPEDIA (June 28, 2024), https://www.investopedia.com/terms/p/panama-papers.asp [https://perma.cc/7K4T-LQTN].

256. *See* Henry Taylor, *5 Charts On The Panama Papers Leaks*, WORLD ECON. F. (Apr. 5, 2016), https://www.weforum.org/agenda/2016/04/5-charts-on-the-panama-papers-leaks/ (last visited Sept. 16, 2024).

clients at the outset or returned more of that data after it was no longer necessary, the harmful effects of this disclosure would have certainly been smaller. The same is true for other accidental disclosures and insider breaches.

Ultimately, requiring lawyers to consider data minimization as part of their duty of data security would require a change in how lawyers think about the client confidences they collect, store, and retain. It need not prevent lawyers from getting the information necessary to provide effective representation or to meet their discovery obligations. The proposal here is to add a step where lawyers ask, "do I need this information?" At the point of collection, this would encourage lawyers to work with clients directly in deciding what confidences to collect and hold digitally. At the point of review, this would encourage lawyers to return documents that they learn are non-responsive or unnecessary to the representation. And at the end of a representation, it would encourage lawyers to return documents that are (a) unnecessary to protect themselves against future malpractice claims or (b) unnecessary to support the creation of future work product.

By integrating data minimization into the lawyer's data security decision-making process, the rules can remain flexible enough to permit lawyers to choose what confidences they need to collect, store, and retain, but would also create a concrete requirement to consider the risks of this collection and retention alongside the benefits. This is a powerful response to the increasingly dangerous world of data security, especially given that it requires no technological knowledge whatsoever. Clients cannot be harmed by confidential information that their lawyers never had or that their lawyers give back. Encouraging lawyers to consider this as part of their process-based duty of data security is an important step in the right direction.

2. Data Segregation

The second process-oriented requirement that should be integrated into the lawyer's duty of confidentiality is "data segregation." Data segregation is the idea that different data should be stored in different locations with different access points, to the extent possible.[257] Not only does this allow "for the creation of separate access rules for sets of data or different groups of users, ensuring that only those who are authorized

257. *What is Data Segregation?*, NEXTLABS (July 31, 2023), https://www.nextlabs.com/what-is-data-segregation/ [https://perma.cc/2S2H-XXSV].

can view, access, remove, or alter the data,"[258] it also limits how much data is stored and is accessible in one place. Like data minimization mitigates harm from a data breach by limiting the quantity of information compromised when a breach occurs, data segregation mitigates harm by limiting the number of access points to confidential data and limiting the quantity of information compromised when one of these access points is breached.[259]

Unlike data minimization, this concept is not entirely foreign to the *Model Rules of Professional Conduct*. Model Rule 1.15 already requires lawyers to segregate their physical property from their client's physical property.[260] This prohibition on comingling is an essential duty in the lawyer-client relationship.[261] Similarly, Model Rule 1.9 requires that "[a] lawyer who has formerly represented a client in a matter or whose present or former firm has formerly represented a client in a matter *shall not thereafter use information relating to the representation to the disadvantage of the former client* . . . ."[262] In practice, this rule requires lawyers and law firms to digitally segregate one client's data from specific conflicted individuals at the law firm or legal organization.

Both of these approaches can and should be introduced into the lawyer's duty of data security. For one, requiring lawyers to segregate personal and professional e-mail and cloud storage devices where practicable is a non-technological way to mitigate the harm from breaches. Although some lawyers surely create this digital separation, many do not. One danger of digital comingling is that it creates more access points for phishing and ransomware attacks. Similarly, although segregating the data of different clients within a law firm or legal organization is admittedly more challenging and costly—both financially and in terms of ease of access—requiring lawyers to at least consider opportunities to avoid a default position of data access for all within the law firm or legal organization would help mitigate accidental access and unauthorized disclosure as well as insider breaches. After all, as illustrated above, one common vulnerability in law firms and legal organizations that

---

258. Abhishek Prabhakar, *All About GDPR Data Segregation*, INTERTRUST TECH. CORP. (Oct. 19, 2021), https://www.intertrust.com/blog/all-about-gdpr-data-segregation/ [https://perma.cc/4YQB-KLGF].

259. *Glossary Definition for "Data Segregation,"* NORDVPN, https://nordvpn.com/cybersecurity/glossary/data-segregation/ [https://perma.cc/4S6H-CU2M] (last visited June 19, 2024).

260. MODEL RULES OF PRO. CONDUCT r. 1.15 (AM. BAR ASS'N 2021) ("A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property.").

261. *Id.*

262. MODEL RULES OF PRO. CONDUCT r. 1.9 (AM. BAR ASS'N 2021) (emphasis added).

makes them susceptible to hacks is when all lawyers and non-legal professionals have access to all client files.[263] Just as law firms have found a way to segregate client data for conflicts purposes, encouraging lawyers and law firms to at least consider ways to segregate client data within the law firm for confidentiality purposes could have a significant impact on mitigating the harm from breaches as well.

3. Data Mapping

The third process-oriented requirement that should be integrated into the lawyer's duty of data security is a principle sometimes referred to as "data mapping."[264] Data mapping is the idea that an entity that takes client information from individuals should know where that data is stored and who has access to it.[265] Like data minimization and data segregation, data mapping is a concrete, technology-agnostic requirement that requires no technical sophistication to implement. Instead, all it requires is good recordkeeping about what technologies are used and who has access to client confidences.

The benefits of a data mapping requirement for law firms and other legal organizations are two-fold. First, requiring individuals to track where client confidences are stored—without judging those decisions—would require lawyers to at least consider when, how, and with whom they share client confidences. This recordkeeping tripwire helps protect against unnecessary sharing of client confidences. Second, requiring this level of recordkeeping helps lawyers protect the access points that exist and respond to data breaches of those access points quickly when they occur. Ultimately, if lawyers "don't know what data they have, where it is located, and how it should be used, then it is hard to imagine how they can keep it secure. Despite the oft-used security metaphor of locks and safes, good security isn't really about locking up data; it's more about looking after data."[266]

---

263. *See supra* section II.A (discussing, among others, the hacks of DLA Piper and the New York Law Department).

264. *The Critical Role of Data Mapping in Integration Projects*, PILOTFISH (Jan. 11, 2023), https://healthcare.pilotfishtechnology.com/critical-role-data-mapping-integration-best-practices/ [https://perma.cc/ERP5-78GW].

265. SOLOVE & HARTZOG, *supra* note 35, at 156–57.

266. *Id.* at 149.

4. Data Security Planning

The fourth process-oriented way to promote risk mitigation is requiring lawyers to adopt a data security plan.[267] In fact, the ABA already recognized the importance of this approach in Resolution 109, which specifically "encourages 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."[268] The problem, as Professor Wald notes, is that this resolution is aspirational, not mandatory.[269]

The benefits of requiring lawyers to adopt a data security (or cybersecurity) plan as a harm mitigation approach are three-fold. First, a data security plan requires individual lawyers—along with the other relevant parties outlined below—to discuss the costs and benefits of adopting specific data security practices. Second, a data security plan allows for a more rapid, intentional, and coordinated response when a data breach occurs. Third, a data security plan requirement is flexible enough to allow different lawyers in different practice areas to make different choices, but concrete enough that the failure to have such a plan could be enforced.

C. People

The second shift necessary to adopt a harm-mitigation-based approach to the lawyer's duty of data security relates to people. In its current form, Model Rule 1.6(c) presumes that data security for the legal profession is a one-person job. That is, in its current form, individual attorneys are solely responsible for taking "reasonable efforts to prevent inadvertent or unauthorized disclosure of, or unauthorized access to," client information.[270] Although Model Rule 1.6(c) and its comments textually permit a lawyer to work with others when making data security decisions, they do not require it.[271] This approach likely made sense when the duty of confidentiality focused exclusively on data secrecy—after all, only the individual lawyer who learned of a client confidence could affirmatively and knowingly disclose that confidence—it makes far less sense in the

267. Wald, *supra* note 6, at 527–28 (arguing for the mandatory adoption of "cybersecurity plans").

268. ABA Resolution 109, *supra* note 6.

269. Wald, *supra* note 6, at 528.

270. MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 2021).

271. Some commentators disagree and argue that, at least by implication, Model Rule 1.6(c) at least requires discussions with clients. *See* Simshaw, *supra* note 189, at 560.

increasingly interconnected digital world of cloud computing. In fact, it is well known that data security failures in the legal profession are rarely the result of the specific decisions of the specific lawyers that take custody of confidential client information.[272] Even when these individual attorneys are a part of the problem, they are rarely the cause of all of the harm from such unauthorized or accidental disclosures.[273] The practice of law today and the associated risks that arise from holding client data digitally are communal in nature, and the lawyer's duty of data security should more fully recognize this reality.

As a result, Model Rule 1.6(c), its comments, and its commentaries should no longer conceive of lawyers as independent data security decision-makers. They instead should see lawyers as data security coordinators, as Formal Opinion 483 already does.[274] More concretely, lawyers should be required to work with three specific groups when making data security decisions. First, lawyers should be required to work with their clients. Engaging clients is critical to balancing the risks and costs of data security efforts because lawyers can better understand the way their clients share data, their choices about what data they share, and the financial resources they are willing to expend to protect the confidentiality of that data. Second, because digital client confidences are rarely accessible only by the individual lawyer that took custody of those confidences, the rules should require consultation and coordination with the other lawyers and non-lawyers in the law firm or legal organization to create an "ethical infrastructure" for protecting client confidences. Third, because lawyers increasingly use third-party tools and vendors to represent and advise their clients, these companies and individuals must also play a more active role in the data security decision-making process. Simply put, "[i]t often takes a village to create a breach,"[275] and it is necessary to include the people that live in that village when making data security decisions.

1. Clients

The first and most important group that lawyers should be required to integrate into the data security decision-making process is clients. There is often an information asymmetry between clients and their lawyers about what confidential information is shared, where it is stored, the relative risks of disclosure, the efforts the client is already taking to prevent that

272. *See supra* section II.A.

273. *See id.*

274. *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 483 (2018).

275. SOLOVE & HARTZOG, *supra* note 35, at 109.

disclosure, and the amount of money that the client is willing to spend for their lawyer to protect against disclosure. Even when clients cannot meaningfully contribute to the conversation about *how* to protect their confidential information, they can contribute to the lawyer's understanding of *what* confidential client information exists and the potential harm from unauthorized or accidental disclosure or access.

That is why it is surprising that neither Model Rule 1.6(c) nor its comments explicitly require that lawyers work with their clients when making security decisions.[276] Formal Opinion 477R suggests that "[a]t the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters," but this guidance does not make clear whether this conversation is mandatory and, if so, what specific topics must be discussed.[277] This is in contrast to many other duties of professional conduct, which require lawyers to gain "informed consent" from their clients when making decisions that impact their clients. The *Model Rules* define informed consent as an "agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct."[278] By contrast, the comments to Model Rule 1.6(c) state that clients "*may* require the lawyer to implement special security measures" or "*may give informed consent* to forgo security measures that would otherwise be required."[279]

Modern data security regimes regularly reject individualized, siloed data security decision-making—and for good reason.[280] Requiring lawyers to work with their clients, instead of presuming that lawyers can reach these conclusions on their own, offers various benefits. Not only does this allow lawyers to make better informed decisions about how to mitigate the risks of disclosure that clients fear, but it also facilitates better alignment of the financial costs and security benefits that come from spending more money and creating more friction in order to adopt more protective policies. In practice, some sophisticated and well-financed clients already demand this level of coordination in their engagement agreements, but the benefits for which these clients pay are not unique to

276. MODEL RULES OF PRO. CONDUCT r. 1.6 cmt 18 (AM. BAR ASS'N 2021) ("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.").

277. *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017).

278. MODEL RULES OF PRO. CONDUCT r. 1.0 (AM. BAR ASS'N 2021).

279. MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 2021) (emphasis added).

280. *See* Cavoukian, *supra* note 249.

them. All clients can benefit from participating in data security discussions.

A simple hypothetical illustrates how introducing clients into data security decision-making responds to the information and cost asymmetry that is a feature of the current approach to the lawyer's duty of data security. Consider a lawyer that wants to use a new piece of software or legal technology. The lawyer might wish to use this new software because they believe it will allow them to better represent the client, more efficiently represent the client, or both. Under the current rules, it is up to the individual lawyer *alone* to determine whether the benefit of using client confidences in coordination with this tool is worth the risk, cost, and potential for harm. By contrast, a rule which requires lawyers to either gain informed consent from clients or even just requires a discussion with clients at the outset of the representation about data security more broadly will give the lawyer additional data points to consider when making their decision: How much risk does this software create? How comfortable is the client with potential disclosure of this specific information? How much cost is the client willing to bear to protect this data? How much benefit does this technology afford? These are all questions which the current rule requires individual lawyers to ask—at least implicitly. Yet, without the client's input, how can the lawyer possibly decide what constitutes a "reasonable" answer?

Although there are any number of ways to require including clients in the data security decision-making process, the most direct would be the introduction of a comment to Model Rule 1.6(c), which requires, instead of merely permits, lawyers to gain informed consent from their clients when making data security decisions. Alternatively, the comment could at least require lawyers to inform clients of their general data security practices during the representation as part of their data security plan. The benefit of more fully including clients—especially in a systemic way as opposed to on a secret-by-secret basis—is that it would reduce the information and expertise asymmetry between lawyer and client that are the cause of many of the specific challenges raised above in Part II. To the extent this level of client consent is already required by Model Rule 1.6(c), as some commentators suggest, then perhaps this requirement is little more than making the implicit explicit—which benefits lawyers, clients, and state bars by clarifying the minimum duties required for any representation.[281] To the extent it is not already required, the profession has much to gain and little to lose by introducing this requirement to the comments to Model Rule 1.6(c).

281. Simshaw, *supra* note 189, at 562.

2. Colleagues

The second critical group of individuals that should be required by the *Model Rules of Professional Conduct* to play a more active role in data security decision-making is the firms and other legal associations in which individual lawyers practice. As almost all of the examples in Part II illustrate, anyone with access to client confidences, or to the digital networks where those client confidences are stored, can be the basis of unauthorized and accidental access or disclosure. In fact, in today's world, the decisions or actions of the individual lawyer that took custody of specific client confidences are rarely the cause of the breach. Bad actors typically do not target one lawyer or legal professional; they instead target everyone who works at a law firm in an attempt to find a single access point to the network.

This was not the case historically. In fact, the other individuals in a law firm or legal organization posed little, if any, threat to the secrecy of client confidences in the pre-digital age. They only pose an extreme threat to the security of these client confidences today because information is often stored on shared digital networks that provide shared digital access. This is why it makes so little sense to frame the duty of data security in ways that focus exclusively on individual lawyers and individual lawyer decision-making. Instead, everyone in a law firm or legal organization should be required to work together in order to provide meaningful digital security to protect client confidences.

In the professional responsibility literature, this firm or organization-wide approach to exercising a duty of professional conduct is known as creating an "ethical infrastructure."[282] As Professors Elizabeth Chambliss and David Wilkins explain,

> The growth of law firms and the emergence of new organizational forms have strained the profession's individualistic approach to lawyer regulation. Because lawyers increasingly practice in large organizations, professional regulation increasingly depends on the development of "ethical infrastructure" within firms; that is, on organizational policies, procedures and incentives for promoting compliance with ethical rules.[283]

This "ethical infrastructure" has been proposed in the context of many professional duties (including conflicts of interest, for example).[284] It is time to bring ethical infrastructure into the duty of confidentiality.

---

282. *See* Elizabeth Chambliss & David B. Wilkins, *Promoting Effective Ethical Infrastructure in Large Law Firms: A Call for Research and Reporting*, 30 HOFSTRA L. REV. 691, 691 (2002).

283. *Id.* at 692.

284. *Id.*

Although the need for this level of coordination presents certain challenges to be sure, this approach could make the duty of security easier to execute.[285] After all, instead of the prevention-based approach which requires lawyer-by-lawyer, document-by-document, and confidence-by-confidence data security decision-making, this requirement would instead encourage a more systematic approach to data security both in terms of policies and architectural protections on a firm level.[286] More than that, this systemwide approach better captures the reality that anyone with access to the networks where client confidences are stored risks disclosing confidences. Of course, requiring the adoption of systemwide data security policies alone is not a foolproof solution. After all, having policies is different from individuals consistently following them. But encouraging practitioners to systematically create and administer these policies on a firm-wide or organization-wide level is, without question, a step in the right direction.

This adoption of an ethical infrastructure approach to the duty of confidentiality brings with it yet another benefit. It encourages lawyers to continuously think about the technologies they use. But unlike the current rule, which relies solely on those decisions, it includes those decisions as part of a broader process and adds the right people to that discussion to make those decisions even more effective.

One critique to this argument might be that the Model Rule 5.1(a) already requires that law firm partners "make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the rules of professional conduct."[287] But, as Professors Chambliss and Wilkins suggest, "research on the regulation of organizations in other contexts suggests that the effectiveness of external regulation depends significantly on the scope and effectiveness of compliance procedures within firms. Thus, the firm [and not the individual lawyers in the firm] remains the central arena—and agent—of regulation."[288] The duty of data security should therefore focus more on this central "arena—and agent—of regulation."[289] This not only better aligns the incentives and risks with the most common data security breach scenarios,[290] but it also recognizes that although data secrecy might be an issue best addressed by the individual lawyers receiving client

285. *See id.*

286. *Id.*

287. MODEL RULES OF PRO. CONDUCT r. 5.1 (AM. BAR ASS'N 2021).

288. Chambliss & Wilkins, *supra* note 282, at 693–94.

289. *See id.* at 694.

290. *See supra* section II.B.

confidences, data security of those confidences requires a firm-wide or organization-wide approach.

3. Contractors

The third and final group of individuals who have a major impact on the security of client confidences but are largely absent from the text of Model Rule 1.6(c) are third-party contractors with whom lawyers work and share confidences. Although Model Rule 5.3 requires lawyers who employ or retain non-lawyers to support client representations to ensure that the conduct of those individuals "is compatible with the professional obligations of the lawyer," this is demonstrated by "direct supervisory authority over the nonlawyer" as opposed to requiring the lawyers to work with these individuals in making decisions.[291]

Although Model Rule 5.3 correctly recognizes that non-lawyer contractors are a common part of contemporary law practice and a major data security risk, it underestimates how to best integrate these third parties into the data security decision-making process. That is, a rule that simply requires lawyers to "directly supervise" these individuals—especially when these are software providers, third-party discovery professionals, freelancers, consultants, and expert witnesses—implies that the lawyers will have a better sense of what efforts should or must be taken to protect client confidences. But it is almost certainly the other way around. In many of these instances, the third party is in the best position to identify data security risks, rectify those risks, and respond in the event of a breach. More than that, to the extent that these individuals have the same or similar access to client confidences as the lawyer—even if they are subject to non-disclosure agreements or other similarly strong contractual obligations—they become yet another access point such that their individual decisions and practices create new and distinct risks that must be considered and addressed.

For example, when the law firms of Jones Day and Goodwin Proctor hired Accellion to help them more securely transfer large quantities of digital data among parties that required access, they were likely trying to create a more secure process for sharing large quantities of client documents.[292] But when Accellion was hacked, so too was the data that those firms sent.[293] This does not mean that the lawyers failed to execute their duty of data security because they used third-party contractors to transmit client confidences. Those contractors almost certainly provided

291. MODEL RULES OF PRO. CONDUCT r. 5.3 (AM. BAR ASS'N 2021).

292. *See* Opfer, *supra* note 135.

293. *Id.*

more secure systems than anything the lawyers themselves could have provided. Nor should contractors that are hacked necessarily be faulted simply because a data security breach occurred. Rather, this is simply a reminder that client data is necessarily stored by third parties—often to make it *more secure*. Therefore, including those individuals in the discussion about how to prepare for and respond to a data breach is essential.

***

Ultimately, outside the legal profession, data security is increasingly understood not as a technological problem with technological solutions but instead as a human problem with human solutions. The human solutions are focused both on incentivizing processes that protect confidential and private information should data security breaches occur and on incentivizing coordination with all relevant parties who can mitigate data security harms before, during, and after a breach. More than that, in the world of cloud computing, questions about data breaches are increasingly seen as questions of if and how to respond rather than how to protect the inevitable from happening.[294] Yet the approach taken by the legal profession over the past twenty-five years has not kept up. Although perhaps the best approach for its time, the legal profession cannot afford to maintain the current technology-based, breach-prevention approach to the lawyer's duty of data security. Instead, as this Part suggests, a better approach to the lawyer's duty of data security is to maintain a regulatory approach that demands reasonableness but reframes that reasonableness as a question of process and people.

CONCLUSION

The duty of confidentiality is a critical component of the attorney-client relationship—and it has been for almost 400 years. That said, the challenges related to that duty have dramatically changed due to the widespread and rapid adoption of cloud-based consumer technology in the contemporary practice of law. The ABA took important steps forward in 1999, 2002, and again in 2012 when it incorporated data security practices into the longstanding duty of confidentiality. Then, state bars took an equally important step by universally adopting the ABA's approach.

---

294. *See* Shuman Ghosemajumder, *You Can't Secure 100% of Your Data 100% of the Time*, HARV. BUS. REV. (Dec. 4, 2017), https://hbr.org/2017/12/you-cant-secure-100-of-your-data-100-of-the-time [https://perma.cc/28WP-G85E].

But what the past two decades prove is that focusing only on preventing unauthorized access is an ineffective, inefficient, and largely unenforceable way to guide lawyers and protect clients. It is, therefore, important to consider new approaches to the lawyer's duty of data security that focus less on technology and individual-lawyer decision-making and more on the process and the people necessary to protect client confidences. This approach better aligns with the purposes of the duty of confidentiality and better responds to the modern realities and challenges of data security.

This is not to say that such changes are likely to occur in the short term. Changes to the *Model Rules of Professional Conduct* come at a slow pace and the relatively recent mass adoption of the current approach by state bars makes further fundamental changes to the duty of confidentiality even less likely at least in the short term. But the world is increasingly on notice of lawyers' failures in the area of data security despite the existence of this professional duty of confidentiality. The world is also facing new confidentiality challenges because of technological innovations like the introduction of generative AI. As a result, a new approach to the lawyer's duty of data security is needed for this new digital reality. It takes only one innovative state bar to spur change. This Article can hopefully serve as a roadmap for a path forward for this change based on principled, expert-informed guidance that retains the flexibility necessary for a rule that must respond to different lawyers, different confidential information, and a constantly evolving technological landscape.

APPENDIX A: SUMMARY OF STATE BAR APPROACHES TO THE DUTY OF DATA SECURITY

States Adopting ABA Model Rule 1.6(c) in Full
Arizona
Arkansas
Colorado
Connecticut
Delaware
Florida
Illinois
Iowa
Kansas
Maine
Massachusetts
Minnesota
Missouri
New Hampshire
New Jersey
New Mexico
New York
North Carolina
North Dakota
Ohio
Oklahoma
Pennsylvania
South Carolina
South Dakota
Tennessee
Utah
Virginia
Washington
West Virginia
Wisconsin
Wyoming

States Omitting Rule 1.6(c) but Maintaining Much or All of the Comments
District of Columbia
Georgia
Hawaii
Idaho
Indiana
Kentucky
Maryland
Mississippi
Nebraska
Vermont

States Adopting Rule 1.6(c) but Omitting Comments 18 and 19
Louisiana
Montana
Nevada
Oregon

States Omitting Rule 1.6(c) and the Comments Entirely but Adopting Reasonableness Concepts by Ethics Opinion
Alabama
Alaska
California
Michigan
Rhode Island
Texas

APPENDIX B: PROPOSED REVISIONS TO THE MODEL RULES OF PROFESSIONAL CONDUCT

Proposal for Model Rule 1.6(c) (additions in bold):

A lawyer shall make reasonable efforts to prevent the **harm from** inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Proposal for Comments 18 and 19:

[18] Paragraph (c) requires a lawyer to act competently to **prevent harm from** ~~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. 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 **harm from such** access or disclosure **regardless of the technologies used**.

Factors to be considered in determining the reasonableness of the lawyer's efforts include **the individuals with whom the lawyer worked when making data security decisions and the processes that they put into place to mitigate harm from such access or disclosures.**

Specifically, in order for efforts to be deemed reasonable under this rule, lawyers must work with their clients, the lawyer and non-lawyer colleagues with whom they are associated, and external third parties that are granted access to client confidences in the course of a representation.

Lawyers also must seek to (1) collect and retain only those client confidences that are reasonably related to a present representation or to facilitate future representations, (2) segregate client data from personal data or the data of other clients where practical, (3) keep a record of the specific people that have access to client data and the specific places that client data is stored, and (4) maintain a current data security plan laying out both the lawyer's process for protecting data that they hold and the response the lawyer will take in the event of a data breach. ~~include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).~~

A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. ~~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 **harm from** 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. 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.