Georgia State University Law Review

Volume 39
Issue 2 *Winter 2023*

Article 13

3-2-2023

The Lawyer's Duty of Tech Competence Post-COVID: Why Georgia Needs a New Professional Rule Now—More Than Ever

Julia Webb
jskiver1@student.gsu.edu

THE LAWYER'S DUTY OF TECH COMPETENCE POST-COVID: WHY GEORGIA NEEDS A NEW PROFESSIONAL RULE NOW—MORE THAN EVER

Julia M. Webb*

ABSTRACT

The American Bar Association (ABA) promulgates the Model Rules for Professional Conduct (Model Rules), which prescribe the behavior with which lawyers must comply in demonstrating competency to practice law. In 2012, the ABA updated Comment 8 to Model Rule 1.1 to require maintaining competence in the "benefits and risks associated with relevant technology," also known as a lawyer's "duty of technological competence." A decade later, the majority of state bar associations have adopted and implemented this language. Georgia, however, remains among the last ten states that have not yet formally adopted the duty of technological competence. The COVID-19 pandemic forced most legal work online, and judges, lawyers, and their clients adjusted to this new normal. With the drastic rise in remote work, no reasonable dispute remains as to whether lawyers should be subject to a duty of technological competence, although questions arise about how this duty should be defined post-pandemic.

* Associate Student Writing Editor, *Georgia State University Law Review*, J.D. Candidate, 2023, Georgia State University College of Law. M.Ed. Literacy Education, Georgia State University College of Education and Human Development, 2019. First—a special thank you to my son, Zachary. You inspire me to be a better person every day. I never imagined that I would homeschool you while attending law school—throughout a global pandemic—but I have been so blessed to be your teacher-mom these past few years. Thank you to all of my friends and family for your support! As a single mama, I am incredibly grateful for my village. Thank you to Professor Andreea Morrison for all that you taught me in your Professional Responsibility course! Special thanks to Professor Jeffery Vagle for your support and guidance throughout the process of writing this note and to all of my brilliant colleagues at the *Georgia State University Law Review* for your dedication and hard work in prepping this note for publication.

This Note argues in favor of Georgia's adoption of the duty of technological competence, proposes changes to the comments accompanying the Georgia Rules of Professional Conduct, and provides practical advice for legal practitioners and their technology departments.

CONTENTS

INTRODUCTION

Globally, governments mandated stay-at-home orders and shut down services in response to the COVID-19 pandemic, fundamentally transforming normalcy by blending work and home for many families.[1] With many industries reporting an increase in productivity and flexibility, an estimated 36.2 million Americans will be working remotely by 2025.[2] The legal profession's increase in remote working gave rise to an unprecedented increase in the use of technology, including virtual practice and videoconferencing.[3] Additionally, some believe that the use of teleconferencing technology in court proceedings may be here to stay.[4] These technologies are now part of a lawyer's everyday practice and are transforming the profession.[5]

1. Grace Hauck, Lorenzo Reyes & Jorge L. Ortiz, *'Stay Home, Stay Healthy': These States Have Ordered Residents to Avoid Nonessential Travel Amid Coronavirus*, USA TODAY, https://www.usatoday.com/story/news/nation/2020/03/21/coronavirus-lockdown-orders-shelter-place-stay-home-state-list/2891193001/ [https://perma.cc/8PD4-G6U3] (Mar. 29, 2020, 5:59 PM). Although the stay-at-home orders varied by state, they "generally require people to avoid all nonessential outings and stay inside as much as possible" with exceptions for essential businesses such as "grocery stores and food production, pharmacies, health care, utilities, shipping, banking, other governmental services, law enforcement, emergency services and news outlets." *Id.*

2. Adam Ozimek, *Economist Report: Future Workforce*, UPWORK, https://www.upwork.com/press/releases/economist-report-future-workforce [https://perma.cc/G8T3-2X9W].

3. 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, 812 (2021). On March 31, 2020, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) temporarily authorized video and teleconferencing for federal proceedings. *Judiciary Authorizes Video/Audio Access During COVID-19 Pandemic*, U.S. CTS. (Mar. 31, 2020), https://www.uscourts.gov/news/2020/03/31/judiciary-authorizes-videoaudio-access-during-covid-19-pandemic [https://perma.cc/D7YY-7PZN]. On March 14, 2020, Georgia suspended most judicial deadlines and encouraged videoconferencing when possible. *Chief Justice Announces Statewide Judicial Emergency*, SUP. CT. GA. (Mar. 14, 2020), https://www.gasupreme.us/judicial-emergency/ [https://perma.cc/EE5U-LM3T].

4. Tom McParland, *Here to Stay: Expect Remote Hearings to Become Post-Pandemic Fixture, Panelists Say*, N.Y.L.J. (July 14, 2021, 4:37 PM), https://www.law.com/newyorklawjournal/2021/07/14/here-to-stay-expect-remote-hearings-to-become-post-pandemic-fixture-rakoff-says/?slreturn=20221004082752 [https://perma.cc/64YH-6K66].

5. Ed Walters, *The Model Rules of Autonomous Conduct: Ethical Responsibilities of Lawyers and Artificial Intelligence*, 35 GA. ST. U. L. REV. 1073, 1073 (2019); John O. McGinnis & Russell G. Pearce, *The Great Disruption: How Machine Intelligence Will Transform the Role of Lawyers in the Delivery of Legal Services*, 82 FORDHAM L. REV. 3041, 3041 (2014). This shift in legal technology is evidenced by "computationally based services" that replace document review in discovery. McGinnis & Pearce, *supra*. These services are on the verge of performing other legal services "from the generation of legal documents to predicting outcomes in litigation." *Id.*

These changes propelled the profession of lawyering into "uncharted territory," and legislatures created new substantive laws to account for the new realities of legal practice.[6] This new legal landscape, and the technologies associated with it, presents a unique opportunity to reform the system and redistribute the benefits and burdens within it, further opening "the doors of justice wide[r] . . . for all people," not just the privileged.[7] Presented with an opportunity to emerge from the pandemic with an improved justice system, lawyers must reflect on their ethical duty to keep up with the pace as technology rapidly changes the world.[8]

In the legal sphere, technological competence can be defined as "an understanding of the technology that a lawyer currently uses in his or her practice, the additional technology available, and the technology that a client or prospective client uses or owns."[9] A lawyer's practice is no longer limited to the technology basics of cloud storage, emails, and e-filing.[10] Technologies such as videoconferencing and document review enhanced by artificial intelligence (AI) have become a part of everyday practice for all attorneys.[11] Once upon a time, a lawyer's use of AI may simply have been for electronic discovery, but its use has expanded into other areas like "legal research, drafting, contract management, and litigation strategy."[12] A lawyer's ethical duty of technological competence changes over time as new technologies emerge and evolve in the legal profession.[13] Because of the State Bar of Georgia's role in shaping ethical standards, it should adopt language to accompany the Georgia Rules of Professional Conduct (Georgia Rules) and provide guidance for technological competence to match

6. William D. Hauptman & Kendra N. Beckwith, *The Duty of Competence in the New Normal*, COLO. LAW., July 2021, at 40, 41.

7. David Freeman Engstrom, *Post-COVID Courts*, 68 UCLA L. REV. DISCOURSE 246, 248 (2020).

8. *See* Hauptman & Beckwith, *supra* note 6, at 43.

9. Kristin L. Yokomoto, *Ethical Duty of Technology Competence*, ORANGE CNTY. LAW., Oct. 2019, at 66, 66.

10. *Id.* at 67.

11. *Id.*; Platt, *supra* note 3; Christopher A. Suarez, *Disruptive Legal Technology, COVID-19, and Resilience in the Profession*, 72 S.C. L. REV. 393, 400, 425 (2020).

12. Walters, *supra* note 5.

13. Yokomoto, *supra* note 9, at 66–67.

the legal profession's ever-changing needs. This Note dives into a lawyer's professional duty of competence with relevant technology, considers the legal pitfalls of using technology in upholding a lawyer's duty, and recommends changes to the Georgia Rules.

Part I explores the background of the professional rules and statutes that govern a lawyer's ethical responsibilities, professional behavior, and duties to clients regarding the evolution of technology in practice. Part II provides an analysis of the litigation, disciplinary actions, and intersection of various rules and statutes governing a lawyer's duty within the technological sphere. Finally, Part III proposes that Georgia adopt new guidance regarding a lawyer's duty of technological competence, given how post-pandemic technology has fundamentally transformed a lawyer's practice. This Note proposes changes to the comments accompanying the Georgia Rules and provides practical advice for legal practitioners regarding the use of relevant technology.

I. BACKGROUND

Technological innovation and transformation are ongoing throughout the legal profession.[14] The profession, however, has a reputation for resisting change and reform.[15] The COVID-19 pandemic forced technological changes like the rise of remote work and the use of videoconferencing in court proceedings, which then became normalized.[16] And these changes are all here to stay.[17] As Big Tech pervades the legal realm, a lawyer's duty of competence in relevant technology is continually evolving.

14. Suarez, *supra* note 11, at 394, 400.

15. James E. Moliterno, *The Trouble with Lawyer Regulation*, 62 EMORY L.J. 885, 885 (2013). After period of crisis and drastic change, legal ethics reform critics repeatedly pose this question: "How can we stay more 'the same' than we already are?" *Id.* at 886. After all, the legal profession's default tendency is to "[p]rotect, preserve, and maintain." *Id.* at 886–87.

16. Suarez, *supra* note 11, at 396–97; Platt, *supra* note 3, at 810–13.

17. *See* Platt, *supra* note 3, at 810–13; Suarez, *supra* note 11, at 394.

A. Emerging Technologies in the Legal Profession

Less than three decades ago, legal practitioners rarely used computers, and there were concerns regarding email security.[18] Email, once an innovative and rarely used messaging system, has become commonplace, and newer technologies, such as those that use predictive analytics, have transitioned into normal use.[19] Although new technologies like legal analytics and AI have been anticipated for years, many lawyers are using these tools unknowingly.[20]

Today, lawyers use tools with predictive coding to assist with document review, drafting, analytics, online dispute resolution, videoconferencing, cloud computing, remote work networks, and email.[21] New technologies provide lawyers with many benefits including "increase[d] efficiency, minimize[d] mistakes, and decrease[d] labor costs."[22] But technology does not come without risks and drawbacks—including hacking, phishing attacks, ransomware, email compromise, malicious insiders, and network vulnerabilities.[23] Even so, with training, careful planning, and expertise, the benefits of emerging technologies significantly outweigh the risks.[24]

18. Suarez, *supra* note 11, at 400; JAMES E. MOLITERNO, THE AMERICAN LEGAL PROFESSION IN CRISIS: RESISTANCE AND RESPONSES TO CHANGE 208 (2013) (discussing South Carolina's 1994 requirement that a client sign an "express waiver" to communicate by email and Iowa's 1996 ruling that email requires encryption and "the client's written consent").

19. Suarez, *supra* note 11, at 400.

20. *Id.* at 400–01 (describing the results of the 2019 ABA Profile of the Legal Profession which "found that only 10% of lawyers thought their firms used AI-based tools" and that "36% of the respondents . . . believed that AI-based tools 'will become mainstream in the legal profession in the next three to five years.'" (quoting AM. BAR ASS'N, ABA PROFILE OF THE LEGAL PROFESSION 52 (2019)).

21. *Id.* at 400.

22. Yokomoto, *supra* note 9.

23. *See id.*; *see also* David G. Ries, *2021 Cybersecurity*, A.B.A. (Dec. 22, 2021), https://www.americanbar.org/groups/law_practice/publications/techreport/2021/cybersecurity/ [https://perma.cc/477W-SPRH]. *See generally* CYBER SEC. LEGAL TASK FORCE, AM. BAR ASS'N, THE ABA CYBERSECURITY HANDBOOK: A RESOURCE FOR ATTORNEYS, LAW FIRMS, AND BUSINESS PROFESSIONALS (Jill D. Rhodes & Robert S. Litt eds., 2d ed. 2018) [hereinafter ABA CYBERSECURITY HANDBOOK] (highlighting cybersecurity practice for risk management in the legal profession).

24. *See* Ries, supra note 23; *see* Darla W. Jackson, *Lawyers Can't Be Luddites Anymore: Do Law Librarians Have a Role in Helping Lawyers Adjust to the New Ethics Rules Involving Technology?*, 105 LAW LIBR. J. 395, 396 (2013).

B. The Evolving State of Ethics in the Legal Profession

A lawyer's duty of technological competence is important.[25] Although not binding, the American Bar Association (ABA) urges courts and lawyers to address the duty of technological competence locally.[26] Lawyers must have a reasonable understanding of the technology used in the profession to make informed decisions about the role technology plays while representing clients.[27] Lawyers are not expected to master every technology, but they are required to maintain a general understanding of risks associated with technologies and must take affirmative steps to avoid harm to clients.[28]

Because of the law's potential to contribute to a just society, lawyers are uniquely positioned to help "promote values and standards."[29] Moving forward from a turbulent political atmosphere and the COVID-19 pandemic, lawyers are equipped to promote positive change as "protectors of the rule of law."[30] According to the ABA, "[m]any of a lawyer's professional responsibilities are prescribed in the Rules of Professional Conduct, as well as substantive and procedural law."[31] Therefore, to fully understand a lawyer's ethical duty, one must understand not only the ABA's Model Rules of Professional Conduct (Model Rules), but also the substantive laws that shape remedies for clients who have been harmed.

25. Suarez, *supra* note 11, at 399.

26. *Id.*

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

28. State Bar of Cal. Standing Comm. on Pro. Resp. & Conduct, Formal Op. 2020-203, at 4 n.4 (2020).

29. Benjamin R. Civiletti, Former U.S. Att'y Gen., The Role of Law and Lawyers in an Ethical Society, Address at the Federal Bar Association Annual Convention (2000), *in* FED. LAW., Nov.-Dec. 2000, at 43, 44.

30. Susan Smith Blakely, *How to Restore Trust for a Profession in Transition*, ABA J. (Jan. 26, 2021, 3:13 PM), https://www.abajournal.com/columns/article/restoring-trust-for-a-profession-in-transition [https://perma.cc/2K8Y-ZWT4**]**.

31. MODEL RULES OF PRO. CONDUCT pmbl. para. 7 (AM. BAR ASS'N 2021).

C. The Rules of Professional Conduct

State malpractice laws and rules created by bar associations complement each other to shape a lawyer's ethical duties.[32] In fact, with only one action, a lawyer may violate a state's professional rules, criminal laws, and commit a tortious act while also facing the consequences of a malpractice suit or court sanctions.[33] The legal profession's self-regulation is "unique . . . because of the close relationship between the profession[,] the processes of government[,] and law enforcement," which is "manifested in the fact that ultimate authority over the legal profession is vested largely in the courts."[34] The ethical considerations associated with "[t]he legal profession's relative autonomy" place a responsibility on attorneys to ensure that the rules that govern lawyers are "in the public interest."[35] Each state's high court enforces their state's rules through disciplinary agencies.[36] Although the professional rules that govern lawyers "are not designed to be a basis for civil liability," they "are designed to provide . . . a structure for regulating conduct through disciplinary agencies."[37]

1. The American Bar Association's Model Rules of Professional Conduct

The Model Rules provide an example of standards for professional responsibility and promote self-regulation within a larger legal and societal context.[38] The ABA maintains that "[a] lawyer, as a member

32. RESTATEMENT (THIRD) OF THE L. GOVERNING LAWS. § 1 cmt. b (AM. L. INST. 2000). According to the Supreme Court of Georgia, "pertinent Bar Rules are relevant to the standard of care in a legal malpractice action." Allen v. Lefkoff, Duncan, Grimes & Dermer, P.C., 453 S.E.2d 719, 721 (Ga. 1995).

33. *See* RESTATEMENT (THIRD) OF THE L. GOVERNING LAWS. § 1 (AM. L. INST. 2000) (noting that lawyers are subject to criminal law, tort law, and malpractice actions at the same time).

34. MODEL RULES OF PRO. CONDUCT pmbl. para. 10 (AM. BAR ASS'N 2021).

35. *Id.* para. 12.

36. LISA G. LERMAN & PHILIP G. SCHRAG, ETHICAL PROBLEMS IN THE PRACTICE OF LAW 21 (concise 4th ed. 2018). Additionally, in "most states, the highest court of the state . . . is responsible for adopting the rules of conduct that govern lawyers." *Id.* (footnotes omitted).

37. MODEL RULES OF PRO. CONDUCT scope para. 20 (AM. BAR ASS'N 2021).

38. *See generally* MODEL RULES OF PRO. CONDUCT pmbl. (AM. BAR ASS'N 2021) (describing the responsibilities of lawyers); MODEL RULES OF PRO. CONDUCT scope (AM. BAR ASS'N 2021) (describing the legal and societal context).

of the legal profession, is a representative of clients, an officer of the legal system[,] and a public citizen having special responsibility for the quality of justice."[39] "As a public citizen, a lawyer should seek improvement of the law, access to the legal system, the administration of justice[,] and the quality of service rendered by the legal profession."[40] By upholding ethical values, lawyers "should further the public's understanding of and confidence in the rule of law and the justice system."[41] The Model Rules provide model language for state bar associations to adopt or modify, and each rule is accompanied by interpretive comments to provide further guidance to the rule.[42] Model Rule 1.1 provides that a lawyer has a duty to "provide competent representation to a client," requiring the "legal knowledge, skill, thoroughness[,] and preparation reasonably necessary for the representation."[43] Comment 8 accompanying Model Rule 1.1 provides: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education[,] and comply with all continuing legal education [CLE] requirements to which the lawyer is subject."[44] Legal professionals and scholars refer to this comment as "the duty of technolog[ical] competence."[45]

2. Georgia's Rules of Professional Conduct

The State Bar of Georgia regulates, enforces, and maintains the Georgia Rules.[46] Like most states, many of the Georgia Rules are

39. MODEL RULES OF PRO. CONDUCT pmbl. para. 1 (AM. BAR ASS'N 2021).
40. *Id.* para. 6.
41. *Id.*
42. *See* MODEL RULES OF PRO. CONDUCT scope para. 21 (AM. BAR ASS'N 2021).
43. MODEL RULES OF PRO. CONDUCT r. 1.1 (AM. BAR ASS'N 2021).
44. *Id.* cmt. 8 (emphasis added).
45. *E.g.*, Robert Ambrogi, *Tech Competence*, LAWSITES, https://www.lawsitesblog.com/tech-competence [https://perma.cc/C9TC-XVEJ]; Platt, *supra* note 3, at 817; Yokomoto, *supra* note 9.
46. GA. RULES OF PRO. CONDUCT r. 4-101 (STATE BAR OF GA. 2021).

modeled after the Model Rules and interpretative guidance.[47] Both the Model Rules and Georgia Rules include a lawyer's general duty of competence.[48] But the Model Rules differ from the Georgia Rules in the specificity of the duty of competence, particularly regarding technology.[49] Unlike Comment 8 to Model Rule 1.1, Comment 6 to Georgia Rule 1.1 omits the language about relevant technology and compliance with CLE requirements.[50] Instead, the commentary only provides that "a lawyer should engage in continuing study and education."[51]

Currently, forty states have formally adopted the Model Rule's duty of technological competence.[52] Figure 1 demonstrates which states have adopted some version of the duty.[53] Some states have adopted the exact language of Comment 8 to Model Rule 1.1,[54] while others have issued additional guidance.[55]

47. *See* LERMAN & SCHRAG, *supra* note 36, at 26–27; *Ethics and Professional Responsibility*, GA. ST. UNIV. COLLEGE OF L. LIBR., https://libguides.law.gsu.edu/c.php?g=253396&p=1689859 [https://perma.cc/Z4NM-LUEF].

48. *Compare* MODEL RULES OF PRO. CONDUCT r. 1.1 (AM. BAR ASS'N 2021) ("A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness[,] and preparation reasonably necessary for the representation."), *with* GA. RULES OF PRO. CONDUCT r. 1.1 (STATE BAR OF GA. 2021) ("A lawyer shall provide competent representation to a client. Competent representation . . . means that a lawyer shall not handle a matter which the lawyer knows or should know to be beyond the lawyer's level of competence without associating another lawyer who the original lawyer reasonably believes to be competent to handle the matter in question. Competence requires the legal knowledge, skill, thoroughness[,] and preparation reasonably necessary for the representation.").

49. *Compare* MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2021) (providing that "a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education[,] and comply with all continuing legal education requirements to which the lawyer is subject"), *with* GA. RULES OF PRO. CONDUCT r. 1.1 cmt. 6 (STATE BAR OF GA. 2021) (providing only that "a lawyer should engage in continuing study and education").

50. *Compare* MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2021), *with* GA. RULES OF PRO. CONDUCT r. 1.1 cmt. 6 (STATE BAR OF GA. 2021).

51. GA. RULES OF PRO. CONDUCT r. 1.1 cmt. 6 (STATE BAR OF GA. 2021).

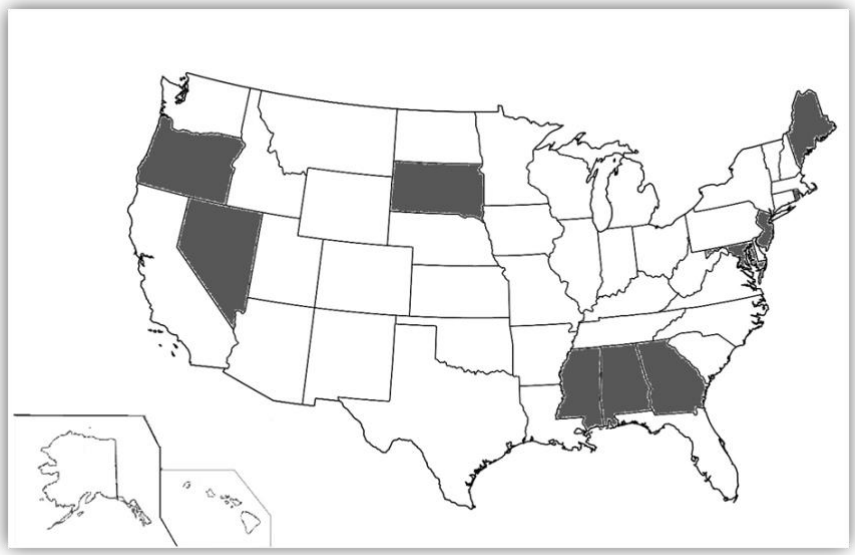
52. Ambrogi, *supra* note 45.

53. *Id.*

54. *See e.g.*, ALASKA RULES OF PRO. CONDUCT r. 1.1 cmt. (ALASKA BAR ASS'N 2021).

55. *See e.g.*, N.Y. RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (N.Y. STATE BAR ASS'N 2022) (including commentary that prescribes a duty to "keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information").

Figure 1. Technological Competence[56]



The states in white have adopted a duty of technological competence, while the darkly shaded states have not yet adopted this standard.[57]

Because so many states have made this leap to explicitly include language regarding relevant technology within the duty of competence, Georgia is positioned to learn from other states in developing its own guidance and standards.

3. The Disciplinary Panel and the Intersection of the Rules

A lawyer's duty of competence is particularly important because many ethical rules intersect within the duty.[58] When a lawyer violates the duty of competence, the lawyer inherently violates multiple rules

56. Ambrogi, *supra* note 45.

57. *Id.*

58. *See* LERMAN & SCHRAG, *supra* note 36, at 193. *See generally* Walters, *supra* note 5 (discussing the intersection between the Model Rules and lawyers' duty while using AI).

because the duty is so broad.[59] This is especially true of the following Georgia Rules and Model Rules: 1.2, specifying the scope of the representation, 1.6, requiring confidentiality, 1.15, requiring safeguarding of client property, 5.1, requiring supervision of lawyers, and 5.3, requiring supervision of nonlawyer employees.[60]

As technology evolves, so does the duty of competence.[61] As such, states are faced with the necessity of addressing the ever-changing needs of the profession, Georgia being no exception.

II. ANALYSIS

Georgia's lawyers must "provide competent representation to a client."[62] Georgia Rule 1.1 explains that "a lawyer shall not handle a matter which the lawyer knows or should know to be beyond the lawyer's level of competence without associating another lawyer who the original lawyer reasonably believes to be competent to handle the matter in question."[63] To practice law in Georgia, one must have the requisite "legal knowledge, skill, thoroughness[,] and preparation reasonably necessary for the representation," or face a maximum penalty of disbarment.[64] Competent representation is not limited to

59. *See, e.g.*, Hauptman & Beckwith, *supra* note 6, at 42, 46 n.15 (providing examples of violations of Rule 1.1 alongside a violation of other rules).

60. *See* GA. RULES OF PRO. CONDUCT r. 1.2, 1.6, 1.15, 5.1, 5.3 (STATE BAR OF GA. 2021); MODEL RULES OF PRO. CONDUCT r. 1.2, 1.6, 1.15, 5.1, 5.3 (AM. BAR ASS'N 2021). *See generally* ABA Comm. on Ethics & Pro. Resp., Formal Op. 498 (2021) (explaining the "ethical duties regarding competence, diligence, and communication, especially when using technology"); ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017) (identifying "the technology risks lawyers face" and various factors "lawyers should consider when using electronic means to communicate regarding client matters"); ABA Comm. on Ethics & Pro. Resp., Formal Op. 483 (2018) (discussing "Model Rules 1.1, 1.6, 5.1, and 5.3, as amended in 2012, [which] address the risks that accompany the benefits of the use of technology by lawyers"); Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2020-300 (2020) (describing rules of professional conduct applicable to lawyers working remotely). As an example of this intersection, to prevent a data breach of confidential client information, a lawyer must take reasonable security precautions to maintain competence in safeguarding clients' property while supervising lawyers and nonlawyers on the necessary proactive protocols. *See generally* ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R (2017) (providing guidance on "Securing Communication of Protected Client Information").

61. *See* Suarez, *supra* note 11, at 444.

62. GA. RULES OF PRO. CONDUCT r. 1.1 (STATE BAR OF GA. 2021).

63. *Id.*

64. *Id.*

substantive "inquiry into and analysis of the factual and legal elements of the problem," but also includes "the requisite knowledge and skill" to practice law, including the "use of methods and procedures meeting the standards of competent practitioners."[65] Because of the legal profession's reliance on technology in the methods and procedures used to practice law, the general duty of competence necessitates technological competence.[66]

Georgia Rule 1.1's commentary is seemingly in conflict with Model Rule 1.1's commentary in that Georgia Rule 1.1 remains silent on whether a lawyer has a duty to understand "the benefits and risks associated with relevant technology."[67] When the Model Rules and the state rules conflict, courts and attorneys are placed in the difficult position of attempting to interpret an attorney's ethical obligations.[68] For example, in *Resolution Trust Corporation v. First of America Bank*, a Michigan lawyer received a privileged and confidential letter inadvertently sent by defendant's counsel.[69] The court found that a Michigan Bar Association Opinion and an ABA Formal Opinion were in conflict and conceded "that precedent did not give clear directions to plaintiff's attorneys."[70] Ultimately, the court followed the ABA's Formal Opinion and ordered the letter destroyed.[71] When rules are in conflict, courts become unpredictable, and with a lawyer's career at

65. *Id.* cmts. 1B, 5.

66. *See generally* Katherine Medianik, Note, *Artificially Intelligent Lawyers: Updating the Model Rules of Professional Conduct in Accordance with the New Technological Era*, 39 CARDOZO L. REV. 1497 (2018) (discussing the integration of AI into legal practice and the need for lawyers to become technologically competent); Katy (Yin Yee) Ho, Note, *Defining the Contours of an Ethical Duty of Technological Competence*, 30 GEO. J. LEGAL ETHICS 853 (2017) (discussing the scope of the duty of technological competence); Jamie J. Baker, *Beyond the Information Age: The Duty of Technology Competence in the Algorithmic Society*, 69 S.C. L. REV. 557 (2018) (discussing the rising use of algorithms in legal practice and the associated duty of technological competence).

67. *Compare* GA. RULES OF PRO. CONDUCT r. 1.1 cmt. 6 (STATE BAR OF GA. 2021), *with* MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2021).

68. *See, e.g.*, Resol. Tr. Corp. v. First of Am. Bank, 868 F. Supp. 217, 220–21 (W.D. Mich. 1994).

69. *Id.* at 218.

70. *Id.* at 219–21. The ABA subsequently released additional guidance on inadvertent disclosure of confidential materials and withdrew Formal Opinion 92-368 in 2005, replacing it with Formal Opinion 05-437. ABA Comm. on Ethics & Pro. Resp., Formal Op. 05-437 (2005).

71. *Resol. Tr. Corp.*, 868 F. Supp. at 220–21.

stake in a disciplinary hearing, the changing technologies necessitate clear guidance on the duty of technological competence.[72]

A. A Lawyer's Duty of Technological Competence

All Georgia lawyers must practice law competently, and technology has become a part of the everyday practice of law.[73] In a technological era, lawyers "would have difficulty providing competent legal services" without performing basic technological functions, such as "us[ing] email or creat[ing] an electronic document."[74]

When the ABA amended its commentary to Model Rule 1.1 regarding a lawyer's need to "keep abreast of changes in the law and its practice," to specifically include "the benefits and risks associated with relevant technology," the Ethics Committee noted this addition "does not impose any new obligations on lawyers."[75] Even though the duty of technological competence is implicit, the Ethics Committee found it "important to make this duty explicit because technology is such an integral – and yet, at times invisible – aspect of contemporary law practice."[76] Therefore, Georgia lawyers already have an implicit duty of technological competence, though neither the Georgia Rules nor the comments explicitly include it.

Since the ABA's 2012 amendments, the ABA and various state bar associations have written opinions to provide further guidance.[77] Because technology is always changing, updating the comments accompanying Georgia Rule 1.1 would at least "offer greater clarity in this area and emphasize the importance of technology to modern law

72. *See id. See generally* sources cited *supra* note 66 (discussing the importance of technological competence in light of technological advancements).

73. GA. RULES OF PRO. CONDUCT r. 1.1 (STATE BAR OF GA. 2021); Suarez, *supra* note 11, at 444.

74. COMM'N. ON ETHICS 20/20, AM. BAR ASS'N, RESOLUTION 105A, at 3 (2012) [hereinafter RESOLUTION 105A], https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a_filed_may_2012.pdf [https://perma.cc/H2MD-MQVM].

75. *Id.*; MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2021).

76. RESOLUTION 105A, *supra* note 74, at 3, 9.

77. *See, e.g.*, State Bar of Mich. Standing Comm. on Pro. Ethics, Formal Op. RI-381 (2020); State Bar of Cal. Standing Comm. on Pro. Resp. & Conduct, Formal Op. 2020-203, at 3–4 (2020), Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2020-300, at 2–3 (2020).

practice."[78] Although the State Bar of Georgia proposed a change to Georgia Rule 1.1's commentary to match the ABA's duty of technological competence in 2019, the Supreme Court of Georgia has not adopted the proposed changes.[79] Even if the Supreme Court of Georgia were to adopt the proposed comment, attorneys need more guidance on what their duty of technological competence entails.[80]

1. The Risks and Benefits of Relevant Technology

Technology makes life easier, whether through e-discovery, basic business management technology, document creation tools, presentation technology, videoconferencing, cloud computing, or much more.[81] Throughout the COVID-19 pandemic, virtual practice became the new normal. And as virtual practice continues post-pandemic, lawyers must engage in an ongoing discussion about the risks and benefits of using technology.[82] As "relevant technology" evolves over time, a lawyer's skill set should evolve with it.[83] However, concerns persist that technology is changing too fast, quickly rendering any guidance from state bar associations obsolete.[84] Specific instructions could help lawyers "apply the current interpretations of the Model Rules to a completely new situation, as they can no longer argue that they are technologically uneducated."[85] With more guidance from the State Bar of Georgia, Georgia's lawyers could enjoy technology's benefits without wondering whether they are complying with their professional duties.

78. RESOLUTION 105A, *supra* note 74.

79. *See* Bob Ambrogi, *Georgia Moves Closer to Adopting Duty of Technology Competence*, LAWSITES (Nov. 4, 2019), https://www.lawsitesblog.com/2019/11/georgia-moves-closer-to-adopting-duty-of-technology-competence.html [https://perma.cc/Z5DW-YVV9].

80. *See* sources cited *supra* note 66 (discussing the importance of technological competence in light of technological advancements).

81. Yokomoto, *supra* note 9; Suarez, *supra* note 11, at 400–17; Platt, *supra* note 3, at 810; Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2011-200, at 2–3 (2011).

82. *See* Platt, *supra* note 3, at 833–34.

83. *See id.* at 832–34.

84. *See id.* at 834.

85. Medianik, *supra* note 66, at 1513.

2. Maintaining Competence

To become technologically competent, a lawyer either (1) knows the technology already, (2) invests the time and effort to learn the technology, or (3) consults with someone else who knows the technology.[86] Thus, "mere exposure to technology is [often] not enough"; technology skills must be maintained.[87] Through technology assessments, lawyers can determine what to target in their own professional learning to maintain competence over time.[88]

Comment 6 to Georgia Rule 1.1 explains that a lawyer's competence, including necessary knowledge and skills, can be maintained by engaging in "continuing study and education."[89] Although Georgia has not yet adopted the additional ABA language to "comply with all [CLE] requirements to which the lawyer is subject," the duty to comply with CLE requirements may be implicit in the text.[90] ABA commentary clarifies that the standard should comply with CLE requirements, which leaves little guesswork at a disciplinary proceeding.[91]

At least two states have taken the ABA's stance on CLE requirements a step further by mandating technology courses for every lawyer.[92] Florida requires three hours of technology CLE every three years,[93] and North Carolina requires lawyers to take an hour each year.[94] Becoming a competent practitioner requires "[s]tudy,

86. Seth M. Wolf & Scott Bennett, *Breaches and Bars: Issues of Legal Ethics in Cybersecurity and Data Breaches (HIT)*, 20180205 AHLA SEMINAR PAPERS 29 (Feb. 5, 2018); *see* Ivy Grey, *How to Meet the Duty of Technology Competence*, LAW TECH. TODAY (June 29, 2017), http://www.lawtechnologytoday.org/2017/06/technology-competence/ [https://perma.cc/LBH8-HYZC].

87. Grey, *supra* note 86.

88. *See id.*

89. GA. RULES OF PRO. CONDUCT r. 1.1 cmt. 6 (STATE BAR OF GA. 2021).

90. *See* MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 8 (AM. BAR ASS'N 2021); RESOLUTION 105A, *supra* note 74.

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

92. *Legal Innovation Regulatory Survey: State Changes of Model Rules*, A.B.A. CTR. FOR INNOVATION, http://legalinnovationregulatorysurvey.info/state-changes-of-model-rules/#Technology [https://perma.cc/LXG9-8CZ9].

93. *Id.*

94. *Id.*

preparation, and [CLE]."[95] "Even highly experienced lawyers must devote themselves to a lifetime of study as ongoing changes in law, technology, and business practices require continual updating of skills."[96] Both the State Bar of Georgia and the Atlanta Bar Association offer some technology-based CLE hours, including an internet legal research course and a three-part webinar on technology.[97] As lawyers participate in CLEs to become more technologically competent, the State Bar of Georgia will need to examine the rules that intersect with the duty of technological competence to provide further guidance.

B. Allocation of Authority with Technology

Georgia Rule 1.2 provides guidance on the scope of representation and the allocation of authority between a lawyer and their client.[98] Pursuant to Georgia Rule 1.2, "a lawyer shall abide by a client's decisions concerning the scope and objectives of representation and . . . shall consult with the client as to the means by which they are to be pursued."[99] Some actions necessary to "carry out the representation" may be "impliedly authorized."[100] A lawyer may "limit the scope and objectives of the representation if the limitation is reasonable under the circumstances and the client gives informed consent."[101] A conflict exists in the "relationship between the obligations created by Model Rule 1.1, addressing competence, and

95. KENNETH L. SHIGLEY & JOHN D. HADDEN, GEORGIA LAW OF TORTS –TRIAL PREPARATION AND PRACTICE § 4:2 (2021 ed.).

96. *Id.*; Ho, *supra* note 66, at 853; Baker, *supra* note 66, at 557.

97. *Internet Legal Research*, STATE BAR OF GA., https://icle.gabar.org/item/internet-legal-research-445932 [https://perma.cc/8SUJ-R5MA]; *CLE Online Library*, ATLANTA BAR ASS'N, https://atlantabar.fastcle.com/store/provider/provider09.php#blank [https://perma.cc/WZ7H-GM5L].

98. GA. RULES OF PRO. CONDUCT r. 1.2 (STATE BAR OF GA. 2021).

99. *Id.*

100. *Id.*

101. *Id.*

Model Rule 1.2(c), addressing the scope of limited services."[102] Because of this, the conclusion might be drawn that "a lawyer may not limit representation to the extent that the lawyer is excused from the obligation to conduct inquiry and analysis," regardless of the intent of drafting and adopting Rule 1.2(c).[103]

Some states have provided guidance on how technology may impact the allocation of authority and scope of representation under Model Rule 1.2 or a state's equivalent rule.[104] Lawyers must consult with their clients under Model Rule 1.2 regarding authorization for extensions, continuances, and any other steps requiring a client's authorization and consent, and this duty extends to various methods of virtual practice.[105] Some states provided guidance on the operation of virtual law offices (VLOs) even before COVID-19 forced many law offices to operate virtually.[106] VLOs permit firms to offer clients who seek "unbundled" services various options to represent them with a limited scope.[107] These "unbundled" services allow the client to decide how much of the lawyer's services they will use.[108] The available services may include "document drafting assistance, document review, representation in dispute resolution, legal advice, case evaluation, negotiation counseling, and litigation coaching."[109] The ABA

102. STANDING COMM. ON THE DELIVERY OF LEGAL SERVS., AM. BAR ASS'N, AN ANALYSIS OF RULES THAT ENABLE LAWYERS TO SERVE SELF-REPRESENTED LITIGANTS 8 (2014) [hereinafter RULES TO SERVE SELF-REPRESENTED LITIGANTS], https://www.americanbar.org/content/dam/aba/administrative/delivery_legal_services/ls_del_unbundling_white_paper_2014.pdf [https://perma.cc/PQ9W-LUZM].

103. *Id.*

104. *See, e.g.*, Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2020-300, at 14 (2020); Ohio Bd. of Pro. Conduct, Advisory Op. 2017-05, at 2 (2017); N.C. State Bar, Formal Op. 2005-10 (2006).

105. Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2020-300, at 13–14 (2020).

106. Ohio Bd. of Pro. Conduct, Advisory Op. 2017-05, at 2 (2017) (defining a VLO as an office that communicates with clients "almost exclusively through secure Internet portals, emails, or other electronic messaging," thereby permitting remote work, reduced overhead, and electronic communications); N.C. State Bar, Formal Op. 2005-10 (2006).

107. Ohio Bd. of Pro. Conduct, Advisory Op. 2017-05, at 2 (2017); N.C. State Bar, Formal Op. 2005-10 (2006).

108. N.C. State Bar, Formal Op. 2005-10 (2006).

109. *Id.*; Ohio Bd. of Pro. Conduct, Advisory Op. 2017-05, at 2 (2017). In contrast, a full bundle of legal services includes "(1) gathering facts, (2) advising the client, (3) discovering facts of the opposing party, (4) researching the law, (5) drafting correspondence and documents, (6) negotiating, and (7) representing the client in court." Forrest S. Mosten, *Unbundling of Legal Services and the Family Lawyer*, 28 FAM. L.Q. 421, 423 (1994).

describes unbundling as "an alternative to traditional, full-service representation" in which

> (1) clients get just the advice and services they need and therefore pay a more affordable overall fee; (2) lawyers expand their client base by reaching those who cannot afford full-service representation but have the means for some services; and (3) courts benefit from greater efficiency when otherwise self-represented litigants receive some counsel.[110]

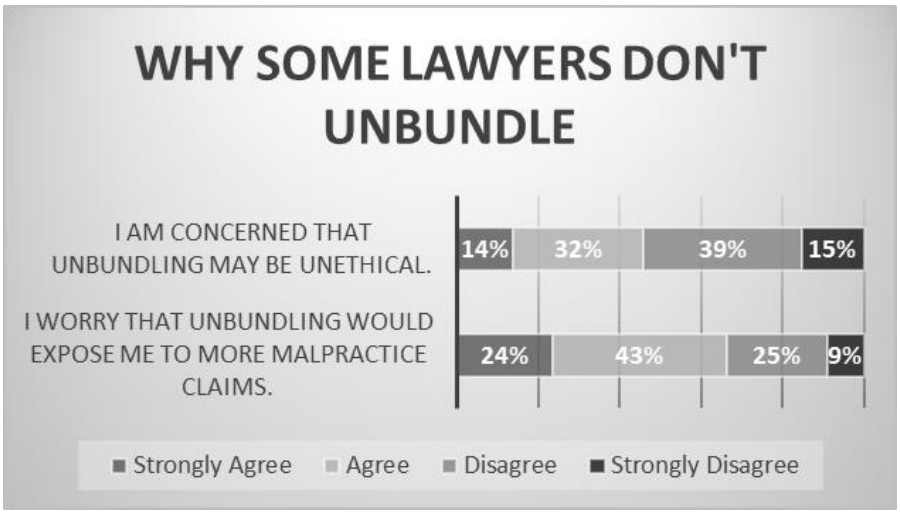
"'[L]imited' and 'full' representation are [not] qualitatively different," however, because many in a lawyer-client relationship make choices from "the full array of *possible* services by selecting some services and rejecting others," which is different from situations where a lawyer "*must* limit their representation."[111] Nevertheless, as highlighted in Figure 2 below, an ABA survey suggests that 67% of lawyers worry that unbundling heightens the risk of malpractice claims while 46% worry about the ethics of unbundling.[112]

110. *Unbundling Resource Center*, A.B.A., https://www.americanbar.org/groups/delivery_legal_services/resources/ [https://perma.cc/5GXM-5QAV].

111. SECTION OF LITIG., AM. BAR ASS'N, HANDBOOK ON LIMITED SCOPE LEGAL ASSISTANCE: A REPORT OF THE MODEST MEANS TASK FORCE 4 & n.7 (2003), https://www.americanbar.org/content/dam/aba/administrative/legal_aid_indigent_defendants/ls_sclaid_handbook_on_limited_scope_legal_assistance.pdf [https://perma.cc/ED5B-Z49M].

112. ABALegalServices, *Lawyer's Use of and Attitudes Toward Unbundling: 2017 Survey Results*, PIKTOCHART, https://create.piktochart.com/output/28644162-multi-state-survey-on-unbundled-legal-services [https://perma.cc/39K3-8GWT].

Figure 2. Ethics Concerns of Lawyers Who Do Not Unbundle[113]



The majority of lawyers who do not unbundle legal services believe unbundling would expose them to malpractice.

The above data suggest that the lack of guidance in the comments regarding the conflict between Model Rules 1.1 and 1.2 (and the associated concerns regarding ethical duties in providing unbundled services) prevents a "full range of [limited-scope] representation options" for clients and discourages competition with document preparation services demanded by clients in the marketplace.[114] The rise in remote work and the convenience in providing unbundled services makes it necessary to clarify Model Rule 1.2 and address ethical concerns about the duty of confidentiality because cloud platforms, videoconferencing technology, and remote networks are already in use.[115]

113. *Id.*

114. RULES TO SERVE SELF-REPRESENTED LITIGANTS, *supra* note 102.

115. *See* sources cited *supra* note 66 (discussing the importance of technological competence in the law in light of technological advancements); Platt, *supra* note 3 (applying the model rules to videoconferencing and remote work); Suarez, *supra* note 11 (discussing the profession's adaptation to the emergence of new technologies during the pandemic); Yokomoto, *supra* note 9.

C. Confidentiality

"Privileged information, confidential information[,] and personal information" are separate but interconnected concepts that lawyers must be familiar with.[116] Unlike the evidentiary rule of privilege, confidentiality of client information is much more far-reaching.[117] In Georgia, lawyers "must maintain in confidence all information gained in the professional relationship with a client . . . unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, or are required by [the Georgia Rules] or other law, or by order of the court."[118] Lawyers may choose to reveal the confidential information when reasonably necessary and warranted by exceptional circumstances.[119] The duty of confidentiality survives the termination of the attorney-client relationship.[120]

Lawyers undoubtedly must maintain competence and use discretion when using technology in their everyday practice to maintain clients' confidentiality, or they could face disciplinary action.[121] The Supreme Court of Georgia and Georgia's disciplinary panel use the ABA's *Standards for Imposing Lawyer Sanctions* as a guide in issuing punishment.[122] When imposing lawyer sanctions, the court considers: "[1] the duty violated; [2] the lawyer's mental state; [3] the potential or actual injury caused by the lawyer's misconduct; and [4] the existence of aggravating or mitigating factors."[123]

116. Joanna L. Storey, *Lawyers Beware: How Data Privacy Protections Differ from Privilege and Confidentiality*, A.B.A. (Dec. 21, 2020), https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2020/how-data-privacy-protections/ [https://perma.cc/K5MS-63M7].

117. *Id.*

118. GA. RULES OF PRO. CONDUCT r. 1.6(a) (STATE BAR OF GA. 2021).

119. *Id.* r. 1.6(b).

120. *Id.* r. 1.6(c).

121. ABA Comm. on Ethics & Pro. Resp., Formal Op. 498, at 3 (2021).

122. *In re* Morse, 470 S.E.2d 232, 232 (Ga. 1996); *see* GA. RULES OF PRO. CONDUCT r. 4-102(c) (STATE BAR OF GA. 2021). *See generally* STANDARDS FOR IMPOSING LAW. SANCTIONS (AM. BAR ASS'N 1986, amended 1992) (providing guidance for sanctions when lawyers engage in misconduct).

123. STANDARDS FOR IMPOSING LAW. SANCTIONS § 3.0, at 16 (AM. BAR ASS'N 1986, amended 1992); *In re Morse*, 470 S.E.2d at 232–33 (finding that aggravating factors were previous disciplinary violations and a mitigating factor was the tragic loss of a partner).

Some violations of confidentiality on technology platforms are obvious. In the disciplinary case *In re Skinner*, a client terminated the relationship with her attorney and subsequently left negative reviews on consumer review websites.[124] The attorney was disciplined by the State Bar of Georgia for, among other things, responding online with "personal and confidential information about the client that [the attorney] had gained in her professional relationship with the client."[125] But some breaches of confidentiality are unintentional, and according to the ABA, "[a] necessary corollary of this duty [of confidentiality] is that lawyers must at least 'make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.'"[126]

1. Data Breaches and Unauthorized Disclosures

For purposes of professional responsibility, a data breach is defined as an "event where material client confidential information is misappropriated, destroyed or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode."[127] The duty of confidentiality and the duty of competence often intersect within the realm of technology concerning data breaches of information systems.[128] For example, a federal court in Missouri found a client's pleadings plausible where the plaintiff stated a claim for breach of implied contract after a law firm "requested, received, created, and/or otherwise obtained highly sensitive, confidential, and proprietary information," which was later accessed by an international hacker

124. *In re* Skinner, 740 S.E.2d 171, 172 (Ga. 2013).

125. *Id.*

126. ABA Comm. on Ethics & Pro. Resp., Formal Op. 498, at 2 (2021) (quoting MODEL RULES OF PRO. CONDUCT r. 1.6(c) (AM. BAR ASS'N 2021)); *see* ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R, at 4 (2017); GA. RULES OF PRO. CONDUCT r. 1.6 cmt. 24 (STATE BAR OF GA. 2021).

127. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 4 (2018).

128. *See* Walters, *supra* note 5, at 1074–82 (discussing the duty of lawyers who use AI under the Model Rules 1.1: Competence and 1.6: Confidentiality).

organization.[129] Not only are these allegations plausible, but a data breach may mean that a firm is subject to extensive discovery and required to produce information about the scope of the breach, the impact of the breach on other clients, and any reports established from external security companies related to the breach.[130] Further, a client may still have a claim if the client's information is stored within an infrastructure with vulnerabilities that leaves a client with simply "a heightened risk of . . . injuries."[131] Figure 3 shows just how prevalent this threat is by displaying the frequency in which firms suffer security breaches resulting from a "lost or stolen computer or smartphone, hack, break-in[,] or exploited website," as reported by the ABA.[132]

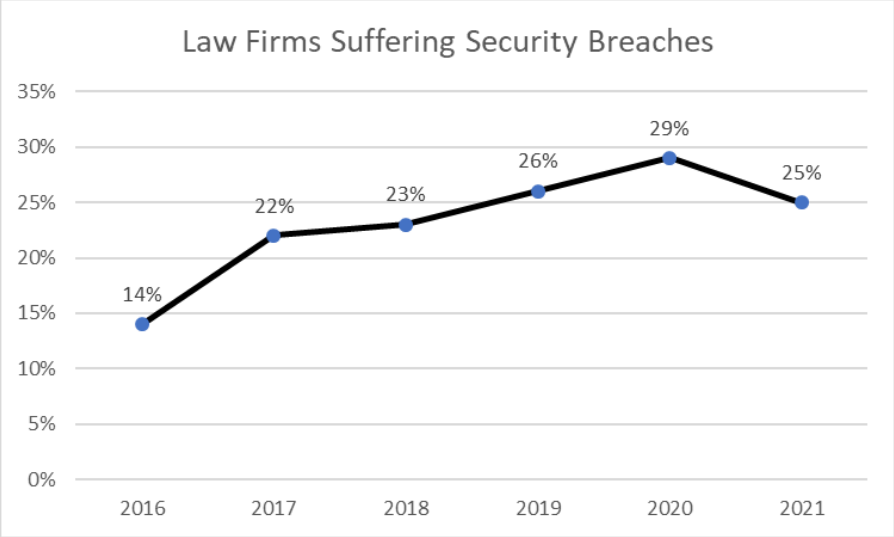
129. Hiscox Ins. Co. v. Warden Grier, LLP, 474 F. Supp. 3d 1004, 1005, 1010 (W.D. Mo. 2020).

130. *See* Guo Wengui v. Clark Hill, PLC, 338 F.R.D. 7, 14–15 (D.D.C. 2021).

131. Shore v. Johnson & Bell, No. 16-CV-4363, 2017 WL 714123, at *1 (N.D. Ill. Feb. 22, 2017).

132. AM. BAR ASS'N, ABA PROFILE OF THE LEGAL PROFESSION 71 (2022) [hereinafter 2022 ABA PROFILE], https://www.americanbar.org/content/dam/aba/administrative/news/2022/07/profile-report-2022.pdf [https://perma.cc/CH65-BNLW]; *see* Ries, *supra* note 23.

Figure 3. Law Firms Suffering Security Breaches[133]



Security breaches have increased significantly since 2016.[134]

When information is compromised, the Model Rules and the Georgia Rules require an analysis of the following nonexclusive factors to determine the reasonableness of the lawyer's efforts to keep clients' information confidential:

> [T]he 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

133. 2022 ABA PROFILE, *supra* note 132; AM. BAR ASS'N, PROFILE OF THE LEGAL PROFESSION 90 (2021) [hereinafter 2021 ABA PROFILE], https://www.americanbar.org/content/dam/aba/administrative/news/2021/0721/polp.pdf [https://perma.cc/TW7X-52NZ].

134. 2022 ABA PROFILE, *supra* note 132; 2021 ABA PROFILE, *supra* note 133.

> clients (e.g., by making a device or important piece of software excessively difficult to use).[135]

The ABA recognizes that there is no "hard and fast rule" to implementing cybersecurity measures, but the factor analysis depends "on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method."[136] This approach "rejects requirements for specific security measures (such as firewalls, passwords, or the like) and instead adopts a fact-specific approach to business security obligations that requires a 'process'" of assessment, identification, implementation, evaluation, and continual updates.[137] Although the ABA rejects specific requirements, it has offered the following guidance for cybersecurity: "Understand the Nature of the Threat," "Understand How Client Confidential Information is Transmitted and Where It Is Stored," "Understand and Use Reasonable Electronic Security Measures," "Determine How Electronic Communications About Client[] Matters Should Be Protected," "Label Client Confidential Information," "Train Lawyers and Nonlawyer Assistants in Technology and Information Security," and "Conduct Due Diligence on Vendors Providing Communication Technology."[138]

Under a fact-based analysis, the ABA concluded that "particularly strong protective measures, like encryption, are warranted in some circumstances."[139] The ABA provides further examples of "reasonable efforts to prevent the inadvertent or unauthorized disclosure"[140] of

135. ABA Comm. on Ethics & Pro. Resp., Formal Op. 498, at 3 (2021) (quoting MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 2021)); GA. RULES OF PRO. CONDUCT r. 1.6 cmt. 24 (STATE BAR OF GA. 2021).

136. ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R, at 4 (2017).

137. Thomas J. Smedinghoff & Ruth Hill Bro, *Lawyers' Legal Obligations to Provide Data Security*, *in* ABA CYBERSECURITY HANDBOOK, *supra* note 23, at 61, 73.

138. ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R, at 6–10 (2017).

139. *Id.* at 5.

140. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 7 (2018) (quoting MODEL RULES OF PRO. CONDUCT r. 1.6(c) (AM. BAR. ASS'N 2021)).

client confidences to include "(i) restoring the technology systems as practical, (ii) the implementation of new technology or new systems, or (iii) the use of no technology at all if the task does not require it."[141]

Although the "reasonableness" standard requires a fact-based inquiry, some states go a step further to "outline some reasonable precautions that attorneys should consider using to meet their ethical obligations."[142] For example, Pennsylvania recognizes the ABA's fact-based approach to reasonableness but also provides "common considerations" for attorneys to consider with respect to cybersecurity for remote workers.[143] Some of these measures include remote data storage and back up, email and laptop encryption, firewalls, antivirus and antimalware software identity verification, virtual private networks (VPNs), two-factor authentication, and the prohibition of conversations around smart devices.[144] Attorneys should also consider that some clients may have their own reasonable preferences for cybersecurity measures.[145]

2. Other Inadvertent Disclosures

With respect to technology and inadvertent disclosures, Model Rule 4.4 states that "[a] lawyer who receives . . . electronically stored information relating to the representation of the lawyer's client and knows or reasonably should know the . . . electronically stored information was inadvertently sent shall promptly notify the sender."[146] Pennsylvania's bar has similarly noted that if information, such as metadata, is inadvertently sent or received, the lawyer must not only notify the sender, but also communicate with the client to "respect

141. *Id.*

142. *See, e.g.*, Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2020-300, at 9–13 (2020) (including, in part, the use of strong passwords, use of secure videoconferencing measures, and avoidance of free internet).

143. *Id.* at 7–8.

144. *Id.*

145. PA. RULES OF PRO. CONDUCT r. 1.6 cmt. 25 (DISCIPLINARY BD. OF THE SUP. CT. OF PA. 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.").

146. MODEL RULES OF PRO. CONDUCT r. 4.4(b) (AM. BAR ASS'N 2021).

the client's authority to control the objectives and means of pursuit," especially if the inadvertent disclosure of metadata may have negative consequences.[147] In fact, several states have formally recognized that clients often want to make informed decisions about what course of action to take after an inadvertent disclosure or a data breach.[148]

D. Safeguarding Client Property

Georgia's lawyers have a duty to safeguard client property, including funds.[149] More specifically, Georgia's lawyers have a duty to "hold funds or other property of clients or third persons that are in a lawyer's possession in connection with a representation separate from the lawyer's own funds or other property."[150] In addition to keeping funds safe for clients, Georgia's lawyers must safeguard any other property in their possession.[151] In Georgia, the standard of care for attorneys with respect to clients' property is that "of a professional fiduciary."[152]

1. Client's Funds

The Georgia Rules outline detailed standards regarding handling a client's money.[153] "Every lawyer who practices law in Georgia, whether . . . a sole practitioner, or as a member of a firm, association, or professional corporation, and who receives money or property on behalf of a client or in any other fiduciary capacity, shall maintain or have available one or more trust accounts as required" by Georgia Rule 1.15 in an "interest-bearing account at an approved institution."[154] However, the State Bar of Georgia provides no guidance for

147. Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2009-100, at 7–8 (2009).
148. *See, e.g., id.*; ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 10–11 (2018).
149. GA. RULES OF PRO. CONDUCT r. 1.15(I) (STATE BAR OF GA. 2021).
150. *Id.*
151. *Id.* The ABA has read Model Rule 1.15 to also include both hard copies and electronic copies of client information as "property" under the rule. *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 12 (2018).
152. GA. RULES OF PRO. CONDUCT r. 1.15(I) cmt. 1 (STATE BAR OF GA. 2021).
153. *Id.* r. 1.15(I)–(III).
154. *Id.* r. 1.15(II).

cybersecurity with respect to the safekeeping of clients' funds under the professional standards for trust accounts.[155]

2. Data Breaches of Financial Information and Identity Theft

"[F]ederal and most states' laws punish identity theft[,] . . . yet, courts have consistently recognized the property rights of business enterprises in their customer lists under both state and federal laws . . . ."[156] Regardless, although a different concept, the collection of personal information "eclipses even client confidences."[157] In Georgia, if individual hackers are identified, law firms may pursue criminal or civil convictions against those hackers who sought to invade the privacy of the firm and its clients under O.C.G.A. § 16-9-93 or the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.[158] However, hackers typically operate in organized crime rings, "often operate remotely," and leave companies "blindsided," making identification of these elusive individuals "incredibly difficult."[159] Data breaches can lead to compromised personal data becoming available on the dark web where criminals can assume new identities and "fraudulently obtain credit cards, issue fraudulent checks, file tax refund returns, liquidate bank accounts, and open new accounts."[160] Although these activities certainly result in financial harm, even the risk of this harm gives rise to a legally cognizable injury.[161]

155. *See* GA. RULES OF PRO. CONDUCT r. 1.15(I)–(III) (STATE BAR OF GA. 2021).

156. Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 404 (2003) (footnotes omitted); *see* Walter W. Miller, Jr. & Maureen A. O'Rourke, *Bankruptcy Law v. Privacy Rights: Which Holds the Trump Card?*, 38 HOUS. L. REV. 777, 779 (2001) (recognizing customer databases as "the most valuable asset").

157. *See* Storey, *supra* note 116.

158. *See* GA. CODE ANN. § 16-9-93 (2022); 18 U.S.C. § 1030.

159. Rishi Iynegar, *Why It's So Difficult to Bring Ransomware Attackers to Justice*, CNN BUS. (July 8, 2021, 12:52 PM), https://www.cnn.com/2021/07/08/tech/ransomware-attacks-prosecution-extradition/index.html [https://perma.cc/9WL6-P2XD].

160. Collins v. Athens Orthopedic Clinic, P.A., 837 S.E.2d 310, 311–12 (Ga. 2019).

161. *Id.* at 311; *see In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1314–17 (N.D. Ga. 2019).

a. An Attorney's Duty in Georgia

"Generally, licensed members of all professions must exercise the degree of skill, prudence, and diligence which ordinary members of the particular profession commonly possess and exercise."[162] In a legal malpractice action, the burden of proof falls upon the plaintiff to prove the three requisite elements: "(1) the employment of the defendant attorney; (2) failure of the attorney to exercise ordinary care, skill, and diligence; and (3) that such negligence was the proximate cause of the damage to the plaintiff."[163] "The test of whether a duty is owed is one of foreseeability," and if a plaintiff has "justifiable grounds" for reliance, a plaintiff is owed a duty.[164] In addition to ordinary neglect of professional duty, a client may assert other non-duplicative claims.[165] Given the potentially huge ramifications of legal malpractice when technological mishaps occur, a lawyer's duty of technological competence is an essential, ongoing component of ethical and professional duty.[166] Because lawyers are held to a higher standard than most ordinary businesses,[167] law firms should prioritize cybersecurity.

162. ERIC JAMES HERTZ & MARK D. LINK, GEORGIA LAW OF DAMAGES WITH FORMS § 30:17 (2021–2022 ed.); Allen v. Lefkoff, Duncan, Grimes & Dermer, P.C., 453 S.E.2d 719, 724 (Ga. 1995) (quoting Tante v. Herring, 439 S.E.2d 5, 8 (Ga. Ct. App. 1993)).

163. HERTZ & LINK, *supra* note 162, § 30:18; DAVID HRICIK & CHARLES R. ADAMS III, GEORGIA LAW OF TORTS § 12:6 (2021).

164. HERTZ & LINK, *supra* note 162, § 30:18; *see, e.g.*, Driebe v. Cox, 416 S.E.2d 314, 315–16 (Ga. Ct. App. 1992) (finding no justifiable grounds for reliance). The duty established by the creation of the attorney-client relationship can be express or implied. Cleveland Campers, Inc. v. R. Thad McCormack, P.C., 635 S.E.2d 274, 276–77 (Ga. Ct. App. 2006); Samnick v. Goodman, 841 S.E.2d 468, 473 (Ga. Ct. App. 2020); Stewart v. McDonald, 815 S.E.2d 665, 671–72 (Ga. Ct. App. 2018); HRICIK & ADAMS III, *supra* note 163.

165. Oehlerich v. Llewellyn, 647 S.E.2d 399, 402 (Ga. Ct. App. 2007) (holding that the plaintiff's "claims for breach of fiduciary duty, breach of contract, and breach of the implied duty of good faith and fair dealing are simply duplications of th[e] legal malpractice claim" because they were based on the breach of a "fiduciary attorney-client relationship").

166. *See* Platt, *supra* note 3, at 818–19; Suarez, *supra* note 11, at 399.

167. *See* GA. RULES OF PRO. CONDUCT r. 1.15(I) cmt. 1 (STATE BAR OF GA. 2021) ("A lawyer should hold property of others with the care required of a professional fiduciary.").

b. Georgia's Economic Loss Rule and Foreseeability

The Supreme Court of Georgia has held that "[t]he 'economic loss rule' generally provides that a contracting party who suffers purely economic losses must [only] seek [a] remedy in contract and not in tort."[168] Thus, no tort remedies are permitted "for purely economic damages arising from a breach of contract."[169] "Where, however, 'an independent duty exists under the law, the economic loss rule does not bar a tort claim because the claim is based on a recognized independent duty of care and thus does not fall within the scope of the rule.'"[170]

In *In re Home Depot, Inc., Customer Data Security Breach Litigation*, the Northern District of Georgia applied Georgia law regarding the foreseeability of a data breach.[171] In 2014, hackers accessed "the personal and financial information of approximately 56 million Home Depot customers," prompting a class action suit comprised of banks that issued compromised credit or debit cards.[172] The banks alleged, among other things, negligence for lack of reasonable security measures.[173] Even though the card issuers and customers had privity of contract, the court found that an independent duty existed "to all the world not to subject them to an unreasonable risk of harm."[174] The court reasoned that the retailer's unreasonable actions, including "disabling security features and ignoring warning

168. Gen. Elec. Co. v. Lowe's Home Ctrs., Inc., 608 S.E.2d 636, 637 (Ga. 2005); *In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2583, 2016 WL 2897520, at *3 (N.D. Ga. May 17, 2016).

169. *In re Home Depot, Inc.*, 2016 WL 2897520, at *3 (quoting Hanover Ins. Co. v. Hermosa Constr. Grp., LLC, 57 F. Supp. 3d 1389, 1395 (N.D. Ga. 2014)).

170. *Id.* (quoting Liberty Mut. Fire Ins. Co. v. Cagle's, Inc., No. 10-CV-2158, 2010 WL 5288673, at *3 (N.D. Ga. Dec. 16, 2010)); *see* GA. CODE ANN. § 9-3-24 (2022) (setting a six-year statute of limitations for breaches of written agreements); Tucker v. Smith, 547 S.E.2d 604, 606 (Ga. Ct. App. 2001) (citing Watkins & Watkins, P.C. v. Williams, 518 S.E.2d 704, 706 (Ga. Ct. App. 1999) (indicating that the statute of limitations for legal malpractice claims is four years)).

171. *See In re Home Depot, Inc.*, 2016 WL 2897520, at *1, *3.

172. *Id.* at *1–2.

173. *Id.* at *2.

174. *Id.* at *3 (quoting Bradley Ctr., Inc. v. Wessner, 296 S.E.2d 693, 695 (Ga. 1982)). This language was later disapproved by the Georgia Supreme Court. Dep't of Lab. v. McConnell, 828 S.E.2d 352, 358 (Ga. 2019).

signs of a data breach, are sufficient to show that the retailer caused foreseeable harm to a plaintiff and therefore owed a duty in tort."[175]

But in the 2019 case of *Department of Labor v. McConnell*, involving an inadvertent disclosure of social security numbers and other personal data, the Supreme Court of Georgia said that "everyone ow[ing] a general duty not to subject others to an 'unreasonable risk of harm'" was nothing more than a misstatement of the law.[176] The court further concluded that this duty was based on a "special relationship," rather than a general duty.[177]

In a 2018 case stemming from another widespread data breach, *In re Arby's Restaurant Group Inc. Litigation*, the Northern District of Georgia anticipatorily distinguished *In re Home Depot* from *McConnell* and found that "even if the *McConnell* decision had any current binding effect, *In re Home Depot* is not expressly inconsistent with *McConnell* because the facts are starkly different."[178] The Northern District of Georgia further noted the *McConnell* court's recognition of Home Depot's "duty to protect" customers' data "in the context of allegations that the defendant failed to implement reasonable security measures to combat a substantial data security risk of which it had received multiple warnings dating back several years and even took affirmative steps to stop its employees from fixing known security deficiencies."[179]

Despite this language in *In re Arby's* leaving the door open for more discussions about the economic loss rule in the context of breaches of personal information, further court decisions seem to uphold the rule in other contexts.[180]

175. *In re Home Depot, Inc.*, 2016 WL 2897520, at *3.

176. *McConnell*, 828 S.E.2d at 358 (quoting *Bradley Ctr.*, 296 S.E.2d at 695). In *McConnell*, the Department of Labor inadvertently disclosed 4,757 social security numbers over email. *Id.* at 356.

177. *Id.* at 358, 359.

178. *In re* Arby's Rest. Grp. Inc. Litig., No. 17-CV-0514, 2018 WL 2128441, at *6 (N.D. Ga. Mar. 5, 2018). In *In Re Arby's*, the complaint alleged, in part, that malware compromised "over 950 restaurants." *Id.* at *2.

179. *Id.* (quoting *McConnell*, 787 S.E.2d at 797 n.4).

180. *See* Murray v. ILG Techs., LLC, 798 F. App'x 486, 488, 492 (11th Cir. 2020) (upholding the economic loss doctrine in a case involving plaintiffs who "were erroneously told they had failed the Georgia bar exam").

c. Reasonableness and the Federal Trade Commission's Authority to Regulate Cybersecurity Practices

Reasonable security measures should be tailored to a firm's needs.[181] *In re Home Depot* provides examples of what courts consider to be unreasonable security measures.[182] There, the court cited, in part, Home Depot's "failure to maintain an adequate firewall," "failure to use up-to-date antivirus software," "failure to encrypt cardholder data," and a general lack of restricted access to sensitive systems.[183] In *In re Arby's*, the plaintiffs survived a motion to dismiss where the complaint alleged that Arby's failed to make reasonable and meaningful improvements to its point of sale systems and networks, such as implementing "point to point encryption" or updating the terminal to include a chip reader.[184] The complaint further alleged that the standards were not compliant with various industry standards and statutes.[185] "[T]he causal chain is not broken" where allegations persist that reasonable security measures were not taken and the "allegations are sufficient to establish that the acts of the third party cyberhackers were reasonably foreseeable."[186] Although the ABA is careful to refrain from providing a definite set of one-size-fits-all standards for

181. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 6 (2018).

182. *In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2583, 2016 WL 2897520, at *1 (N.D. Ga. May 17, 2016).

183. *Id.* The National Institute of Standards and Technology (NIST) defines some of the key terms from the above case. Firewalls "control[] the flow of network traffic between networks or hosts that employ differing security postures." *Firewall*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/firewall [https://perma.cc/5U4A-DUXG]. Antivirus software "monitors a computer or network to identify all major types of malware and prevent or contain malware incidents." *Antivirus Software*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/Antivirus_Software [https://perma.cc/Y2HZ-L7WL]. Encryption "convert[s] plain text into cipher text to prevent anyone but the intended recipient from reading that data." *Encryption*, NAT'L INST. OF STANDARDS & TECH, https://csrc.nist.gov/glossary/term/encryption [https://perma.cc/BXT8-8BBK].

184. *In re Arby's Rest. Grp. Inc.*, 2018 WL 2128441, at *2, *14.

185. *Id.* at *2.

186. *In re* Equifax, Inc., Customer Data Sec. Breach Litig., 362 F. Supp. 3d 1295, 1320 (N.D. Ga. 2019).

cybersecurity solutions,[187] the allegations in cases that survived summary judgment are helpful to understand what is reasonable for competent lawyers as advocates for their retailer clients and in planning their own firm's security measures.

Even more important than being familiar with state law, lawyers should be familiar with the Federal Trade Commission Act (FTCA) and any related cybersecurity settlements.[188] The FTCA prohibits "unfair or deceptive [methods and] acts or practices in or affecting commerce."[189] The Federal Trade Commission (FTC) uses this language to bring administrative actions "against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers."[190] The majority of these actions "end[] in settlement."[191]

In 2015, hotel giant Wyndham Worldwide Corporation challenged the FTC's "authority to regulate cybersecurity under the unfairness prong" of subsection 45(a) of the FTCA.[192] Wyndham's computer systems were hacked three times during 2008 and 2009, resulting in "at least $10.6 million in fraud loss" and impacting 619,000 consumers.[193] The FTC claimed Wyndham engaged in unfair practices, such as "stor[ing] payment card information in clear readable text," using default passwords or ones that could be "easily guessed," and using at least one "out-of-date operating system."[194] Additionally, the FTC claimed some of Wyndham's inactions, such as failure to use firewalls, restrict third-party vendors, conduct security

187. *See* ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 6 (2018); MODEL RULES OF PRO. CONDUCT r. 1.1 cmt. 5 (AM. BAR ASS'N 2021) ("Competent handling of a particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners.").

188. *See* Jon L. Mills & Pedro M. Allende, *FTC Consent Decrees Are Best Guide to Cybersecurity Policies*, FLA. BUS. REV., https://www.law.com/dailybusinessreview/almID/1202737711574/#ixzz3niw5jHOf [https://perma.cc/P24K-LAFV] (Sept. 21, 2015).

189. 15 U.S.C. § 45(a)(1).

190. FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015).

191. *Id.*

192. *Id.*

193. *Id.* at 241–42.

194. *Id.* at 240–41.

investigations, or "follow proper incident response procedures," constituted unfair practices.[195] Although not discussed on appeal, the FTC "also raise[d] a deception claim alleging that since 2008 Wyndham ha[d] published a privacy policy on its website that overstate[d] the company's cybersecurity."[196] On appeal, Wyndham argued that the meaning of "'unfair' impose[d] independent requirements" outside the language of the statute and that Congress intended to exclude cybersecurity from the FTCA.[197] Despite Wyndham's challenge, the Third Circuit upheld the FTC's regulatory authority under the broad language of subsections 45(a)(1) and (n).[198]

Additionally, Wyndham argued that "the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow" to avoid liability.[199] The court found Wyndham's argument unpersuasive given that hackers accessed the systems three times in two years, and "certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court *could* find that its practices fail the cost-benefit analysis" of subsection 45(n).[200] Further, the Third Circuit concluded that proper notice of sufficient cybersecurity measures can be found in the FTC's numerous consent decrees, guidebooks, and other publications.[201]

Because of the FTC's authority in the area of cybersecurity, "[e]xecutives tasked with cybersecurity within their companies should familiarize themselves with the body of FTC consent decrees publicly available on its website and monitor new actions being filed to better understand the evolution of what the FTC thinks is appropriate."[202] Not only should firms become familiar with these consent decrees, but they should also conduct ongoing research to understand "[t]he evolving

195. *Id.* at 241 (internal quotation marks omitted).
196. *Wyndham Worldwide Corp.*, 799 F.3d at 241.
197. *Id.* at 244, 247.
198. *Id.* at 259; Mills & Allende, *supra* note 188; *see* 15 U.S.C. § 45(a)(1), (n).
199. *Wyndham Worldwide Corp.*, 799 F.3d at 249.
200. *Id.* at 255–57.
201. *Id.* at 256–57. The Third Circuit compared similarities in the FTC's complaint against Wyndham to a previous complaint against CardSystems Services (CSS) to show Wyndham had fair notice based on prior FTC actions. *Id.* at 258 tbl.
202. Mills & Allende, *supra* note 188.

and complex regulatory environment" of cybersecurity's best practices.[203] Accordingly, lawyers should familiarize themselves with the following recommendations from the FTC consent decrees: "[s]tart with security," "[c]ontrol access to data sensibly," "[r]equire secure passwords and authentication," "[s]tore sensitive personal information securely and protect it during transmission," "[s]egment your network and monitor who's trying to get in and out," "[s]ecure remote access to your network," "[a]pply sound security practices when developing new products," "[m]ake sure your service providers implement reasonable security measures," "[p]ut procedures in place to keep your security current and address vulnerabilities that may arise," and "[s]ecure paper, physical media, and devices."[204]

The wealth of information published by the FTC is important for competent lawyers to determine what constitutes reasonable security measures for their firms as well as the businesses they advise.[205]

E. Supervision of Lawyers and Nonlawyers

Smaller firms often outsource technology experts while larger firms tend to hire full-time information technology staff who share the responsibility of maintaining client confidences.[206] When a firm's third-party software vendor is subject to a data breach, questions may arise over who to hold responsible.[207] Regardless, cloud computing is

203. *Id.*

204. FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS 2–14 (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf [https://perma.cc/Y2HC-H3BT].

205. The FTC maintains a full body of work summarizing key enforcement actions and connecting businesses with practical advice. *See Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/datasecurity [https://perma.cc/3868-HE5F].

206. *See* Trevor Bell, *What Large and Small Firms Can Teach Each Other in Legal Tech Implementations*, LEGALTECH NEWS (Apr. 6, 2020, 7:00 AM), https://www.law.com/legaltechnews/2020/04/06/what-large-and-small-firms-can-teach-each-other-in-legal-tech-implementations/ [https://perma.cc/F3KX-G9HU].

207. *See* David Thomas, *Lawsuits Mount for Vendor Linked to Jones Day, Goodwin Procter Data Breaches*, REUTERS LEGAL (Feb. 25, 2021, 8:40 PM), https://today.westlaw.com/Document/I77d2f8c077ab11eb91c9f2c154ea134a/View/FullText.html?transitionType=SearchItem&contextData=(sc.Default) [https://perma.cc/H8ST-KZD6] (providing detail on a widely publicized data breach).

subject to Model Rules 5.1 and 5.3 regarding an attorney's supervision of others, so lawyers should ensure that information is managed by "competent" third-party vendors.[208]

1. Supervision of Lawyers

Lawyers with managerial or direct supervisory authority in a law firm must "make reasonable efforts to ensure" that the firm and other lawyers that they supervise comply with the Georgia Rules.[209] Lawyers in supervisory roles are responsible for other lawyers' violations of the Georgia Rules if they knowingly ratify any misconduct or "fail[] to take reasonable remedial action" when the misconduct's consequences can still be mitigated.[210] Virtual practice, whether due to the COVID-19 pandemic or otherwise, does not change a lawyer's duty.[211] Internal policies and procedures should "detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property[,] and ensure that inexperienced lawyers are properly supervised."[212] Therefore, "lawyers must employ reasonable efforts to monitor the technology and office resources connected to the internet, external data sources, and external vendors providing services relating to data and the use of data."[213]

Without protocols in place, a lawyer might not identify a breach, let alone decide whether other regulatory and legal provisions require further action.[214] This duty of care for electronically stored property and information is akin to the lawyer's responsibility to ensure that everyone in the firm protects "the security of paper files and actual client property."[215] A cyberattack might not be immediately detected,

208. Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2011-200, at 7 (2020).
209. GA. RULES OF PRO. CONDUCT r. 5.1(a)–(b) (STATE BAR OF GA. 2021).
210. *Id.* at r. 5.1(c).
211. ABA Comm. on Ethics & Pro. Resp., Formal Op. 498, at 3 (2021).
212. GA. RULES OF PRO. CONDUCT r. 5.1 cmt. 2 (STATE BAR OF GA. 2021).
213. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 5 (2018) (footnote omitted); *see* ABA Comm. on Ethics & Pro. Resp., Formal Op. 08-451, at 1 (2008).
214. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 5 (2018).
215. *Id.*

even with extraordinary measures taken by partners in supervision of others, because cyber criminals can be elusive.[216] But "when a lawyer does not undertake reasonable efforts to avoid data loss or to detect cyber-intrusion, and that lack of reasonable effort is the cause of the breach," the potential for an ethics violation arises.[217]

Reasonable measures include the creation of an incident response plan, and the ABA adamantly encourages adopting a plan "before a lawyer is swept up in an actual breach."[218] Although the ABA is reluctant to give specific advice, as each "plan should be tailored" to each practice, it outlines common features of incident response plans as follows:

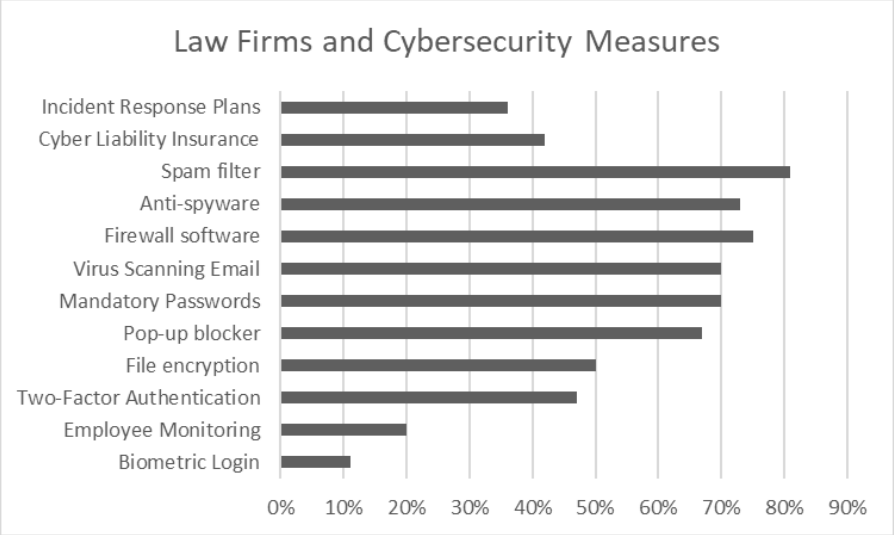
> The incident response process should promptly: identify and evaluate any potential network anomaly or intrusion; assess its nature and scope; determine if any data or information may have been accessed or compromised; quarantine the threat or malware; prevent the exfiltration of information from the firm; eradicate the malware, and restore the integrity of the firm's network.
>
> Incident response plans should identify the team members and their backups; provide the means to reach team members at any time an intrusion is reported; and define the roles of each team member. The plan should outline the steps to be taken at each stage of the process, designate the team member(s) responsible for each of those steps, and the team member charged with overall responsibility for the response.[219]

216. *Id.* at 5–6.
217. *Id.* at 6.
218. *Id.*; *see* Alan Charles Raul & Michaelene E. Hanley, *Large Law Firms*, *in* ABA CYBERSECURITY HANDBOOK, *supra* note 23, at 187, 202.
219. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 6–7 (2018) (quoting Steven M. Puiszis, *Prevention and Response: A Two-Pronged Approach to Cyber Security and Incident Response Planning*, 24 PRO. LAW., no. 3, 2017, at 25, 26).

In implementing a plan post-breach, lawyers with supervisory roles should (1) identify a point person, (2) mitigate damage, and (3) communicate with other relevant parties.[220]

Figure 4 displays data from self-reported cybersecurity measures currently in law firms based on the ABA's most recent profile of the profession.[221]

Figure 4. Law Firms and Cybersecurity Measures[222]



Often, the likelihood of having any of these measures in place is a function of the firm's size.[223] **For example, 80% of firms with more than 100 attorneys reported having an incident response plan compared to 12% of solo practitioners.**[224]

A lawyer's duty of supervision requires having basic technological competence and employing experts when necessary to assist in such

220. *See* Rachel Aghassi & Ahmed Javaid, *Fortifying the Firm: How to Confront Digital Threats to the Modern Law Firm*, NYSBA INS. FOCUS BLOG (Aug. 2, 2021, 7:04 AM), https://usiaffinity.typepad.com/nysba_insurance_focus/2021/08/fortifying-the-firm-how-to-confront-digital-threats-to-the-modern-law-firm-.html [https://perma.cc/U8RX-9ENQ].

221. 2022 ABA PROFILE, *supra* note 132, at 72; Ries, *supra* note 23.

222. 2022 ABA PROFILE, *supra* note 132, at 71–72; Ries, *supra* note 23.

223. Ries, *supra* note 23.

224. *Id.*

duty, whether the duty arises at a law firm or through remote work.[225] In regards to virtual practice, firms employing a "bring-your-own-device (BYOD) policy" should carefully supervise lawyers to "ensure that security is tight" through strong passwords, VPN access, updated systems, phishing training, remote wiping capabilities, and system inaccessibility to nonemployee household members.[226] When working remotely, the lawyer must still be able to account for basic trust accounting records, send and receive paper mail, and properly communicate with clients.[227]

2. Supervision of Nonlawyer Assistants

When nonlawyers are employed, retained by, or associated with Georgia lawyers, "reasonable efforts" must be made to ensure compliance with the Georgia Rules and other "professional obligations of the lawyer."[228] Similar to the supervision of fellow lawyers, lawyers must refrain from ratifying or failing to mitigate nonlawyers' misconduct.[229]

a. Training Staff

The duty to supervise nonlawyer assistants "requires regular interaction and communication with, for example, . . . legal assistants[] and paralegals."[230] Nonlawyers at a firm may also include "internal technical support staff," who are often the staff that lawyers

225. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 2 n.7 (2018); State Bar of Cal. Standing Comm. on Pro. Resp. & Conduct, Formal Op. 2020-203, at 4 n.4 (2020); *see* ABA Comm. on Ethics & Pro. Resp., Formal Op. 477R, at 10 (2017) ("Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education."); ABA Comm. on Ethics & Pro. Resp., Formal Op. 498, at 3 (2021); MODEL RULES OF PRO. CONDUCT r. 1.1 cmts. 2, 8 (AM. BAR ASS'N 2021).

226. ABA Comm. on Ethics & Pro. Resp., Formal Op. 498, at 7 (2021).

227. *Id.* at 7–8.

228. GA. RULES OF PRO. CONDUCT r. 5.3(b) (STATE BAR OF GA. 2021).

229. *Compare id.* r. 5.1(c), *with id.* r. 5.3(c).

230. ABA Comm. on Ethics & Pro. Resp., Formal Op. 498, at 6–7 (2021). This communication must be so "direct and constant" that the State Bar of Georgia prohibits lawyers from attending real estate closings remotely via telephone conference with a paralegal and the client. Ga. Sup. Ct., Formal Advisory Op. 00-3 (2000).

in big firms turn to when technology problems arise.[231] Frequent practical training through employee simulation can be helpful because technologies are ever-evolving.[232] Nonlawyer staff should be educated on how to handle sensitive data, detect cyberattacks, and take appropriate action.[233] The training "should be tailored to the specific needs of each firm" and the type of sensitive data the firm handles.[234]

b. Outsourced Technology Services

Nonlawyer assistants also include vendors or technology consultants who support a firm.[235] The ABA emphasizes that "[t]he lawyer must ensure that all of these individuals or services comply with the lawyer's obligation of confidentiality and other ethical duties."[236] With the rise in remote work, vendors for cloud services provide many benefits, "including anytime, anywhere access, low cost of entry, predictable monthly expenses," elimination of software management requirements, and in some cases, even better security than in the office.[237] Outsourced technology services require supervising lawyers to do their homework in seeking out vendors or outside help to ensure competence, and "lawyer[s] should consider investigating the security of the provider's premises, computer network, and perhaps even its recycling and refuse disposal

231. Mark Rosch, *2020 Technology Training*, A.B.A. (Nov. 16, 2020), https://www.americanbar.org/groups/law_practice/publications/techreport/2020/techtraining/ [https://perma.cc/8TFD-FL3V]; Sofia Lingos, *2021 Technology Training*, A.B.A. (Dec. 8, 2021), https://www.americanbar.org/groups/law_practice/publications/techreport/2021/techtraining/ [https://perma.cc/T8QP-B693].

232. Temitope Ige & Opeyemi Ilesanmi Esther, Cybersecurity: New Standards, New Expectations for the 21st-Century Legal Practitioner (Feb. 3, 2020) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3531268 [https://perma.cc/YG4F-JL4M].

233. *Id.*

234. *Id.*

235. *See* Rosch, *supra* note 231.

236. ABA Comm. on Ethics & Pro. Resp., Formal Op. 498, at 7 (2021) ([L]awyers should consider use of a confidentiality agreement, and should ensure that all client-related information is secure, indexed, and readily retrievable." (footnote omitted)).

237. Dennis Kennedy, *2020 Cloud Computing*, A.B.A. (Oct. 26, 2020), https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cloudcomputing/ [https://perma.cc/9L2H-E3NQ].

procedures."[238] With respect to technology vendors, the ABA provides resources to help facilitate communication regarding technologies for vendors, and such resources are important for legal practitioners to use in the course of business.[239]

III. PROPOSAL

Realistically, the Model Rules cannot be amended to accommodate every minor change in law practice or technology.[240] But a global pandemic that has fundamentally shifted the law's use of technology warrants an update to "continue to inform and guide lawyers' actual practice and avoid becoming antiquated."[241] Furthermore, clarity will serve as a guidepost to "manage the tension between [the lawyer's] duty of zealous advocacy and staying within the boundaries of proper legal ethics."[242] Because Georgia currently lacks ethics opinions on technological competence, lawyers are more likely to find themselves either "questioning the application of an ethics rule to a certain situation not found in any reported case" or being left to "interpret their own ethical obligations."[243]

To protect the public interest in a lawyer's duty of competent representation, the State Bar of Georgia should address the ambiguities in the Georgia Rules. First, by stating that an express duty of technological competence exists, the state will eliminate confusion

238. ABA Comm. on Ethics & Pro. Resp., Formal Op. 08-451, at 2–3 (2008).

239. *See generally* CYBERSECURITY LEGAL TASK FORCE, AM. BAR ASS'N, VENDOR CONTRACTING PROJECT: CYBERSECURITY CHECKLIST (2d ed. 2021).

240. Eli Wald, *Legal Ethics' Next Frontier: Lawyers and Cybersecurity*, 19 CHAP. L. REV. 501, 526 (2016).

241. *Id.*; Platt, *supra* note 3, at 826–27 ("Significant advances in technology and its integration into the practice of law have spurred changes to the Model Rules in the past[,] and the transition to an increasingly remote practice conducted over videoconferencing platforms and the risk of unauthorized disclosure of client information associated with this transition is a modern circumstance that necessitates an update to the Model Rules." (footnote omitted)).

242. Mitchell James Kendrick, Comment, *A Shot in the Dark: The Need to Clearly Define a Lawyer's Obligations Upon the Intentional Receipt of Documents from an Anonymous Third Party*, 123 PENN ST. L. REV. 753, 754, 776–77 (2019).

243. Platt, *supra* note 3, at 827.

regarding an implied duty of technological competence.[244] The Georgia bar should also clarify what that duty entails.[245] Furthermore, by addressing the rules that intersect with the duty of technological competence, like Rules 1.2, 1.6, 1.15, 5.1, and 5.3, Georgia's lawyers will understand the scope of their duty of technological competence, their responsibility to supervise others with that same duty, and their duty to protect property and client confidences.

A. Tech Competence

The State Bar of Georgia should, at minimum, adopt the ABA's language requiring lawyers to understand "the benefits and risks associated with relevant technology."[246] The practice of law is largely technology-dependent and has only continued to become more so within the last few years.[247] If the Georgia bar were to highlight what the primary "benefits and risks" are, as well as what "relevant technology" refers to, that clarification would prove invaluable to attorneys who are struggling to determine their ethical obligations.[248] Therefore, the following statements are proposed revisions to Comment 8 accompanying Georgia Rule 1.1.

> Proposed Comment: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all [CLE] requirements to which

244. *See* RESOLUTION 105A, supra note 74 ("[T]he amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.").

245. *See* Platt, *supra* note 3, at 828 (proposing comments to the Model Rules and arguing that "[v]ague rules . . . lead to increased conflict when it comes to interpretation of these rules"); *see also* Wald, *supra* note 240, at 527 (arguing that the "[Model] Rules' approach to cybersecurity must recognize and effectuate an affirmative duty to reasonably protect clients' information and develop a helpful definition of reasonableness that encompasses an obligation to protect client information from criminal activity").

246. *See* RESOLUTION 105A, *supra* note 74, at 2.

247. *See* Medianik, *supra* note 66, at 1531; McParland, *supra* note 4.

248. *See* Platt, *supra* note 3, at 827, 831–36.

> the lawyer is subject."[249] Additionally, a lawyer's assessment of the benefits and risks of practice technology must include: the firm's size, the firm's clientele, cost effectiveness, efficiency, accessibility, security measures to match the sensitivity of the information stored, training measures, responsibilities in a data breach, and compliance with state and federal laws.[250] Relevant technology includes all technologies used by the lawyer, as well as similarly situated lawyers in the scope of practicing law to provide services, communicate, store, or transmit information.[251] Lawyers may consult experts in the field as necessary to maintain technological competence.[252]

In addition to clarifying the "benefits and risks of relevant technology," Georgia should require technology-based CLE credits. Although Florida and North Carolina are in the minority of states that require technology training, the practice of law's increasing dependence on technology only exacerbates the necessity of such learning.[253] Not only do attorneys need to understand their own technology, but by being "continuously conscious of improvements in technology," attorneys will be better positioned to meet the needs of modern-day competent and ethical practice.[254]

---

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

250. *See* Smedinghoff & Bro, *supra* note 137, at 73–87 (analyzing "reasonable security"); *see* Platt, *supra* note 3, at 832 (discussing the benefits and risks of videoconferencing in contemporary legal practice).

251. *See generally* ABA CYBERSECURITY HANDBOOK, *supra* note 23 (providing practical advice for lawyers in large firms, small firms, in-house, government, and public interest).

252. State Bar of Cal. Standing Comm. on Pro. Resp. & Conduct, Formal Op. 2020-203, at 4 n.4 (2020); State Bar of Ariz. Rules of Pro. Conduct Comm., Ethics Op. 09-04 (2009); Peter Geraghty & Lucian T. Pera, *Lawyers' Obligations to Provide Data Security Arising from Ethics Rules and Other Law*, *in* ABA CYBERSECURITY HANDBOOK, *supra* note 23, at 115, 124.

253. *See* Jeff Cox, *Why Every State Should Require Technology CLEs*, LAW TECH. TODAY (May 20, 2019), https://www.lawtechnologytoday.org/2019/05/why-every-state-should-require-technology-cles/#:~:text=As%20such%2C%20the%20technology%20CLE%20requirement%20is%20not,order%20to%20promote%20increased%20technological%20competence%20among%20lawyers [https://perma.cc/DZU3-VFLP]; Medianik, *supra* note 66, at 1531.

254. Ash Mayfield, Comment, *Decrypting the Code of Ethics: The Relationship Between an Attorney's Ethical Duties and Network Security*, 60 OKLA. L. REV. 547, 563 (2007).

B. Scope of Representation in a Remote Work World

Modern-day practice means that lawyers are working remotely and using more cloud storage, more e-discovery techniques, and more videoconferencing.[255] New technologies have undoubtedly made it easier to provide limited-scope representation to clients.[256] The difficulty lies in maintaining competence while expanding the availability of legal services through new technologies.[257] The State Bar of Georgia should clarify the role of technology and virtual practice in limited-scope representation. A new proposed comment to accompany Georgia Rule 1.2 reads as follows.

> Proposed Comment: When a client gives informed consent and solely wants a lawyer to provide either legal information or document preparation through limited-scope representation, such arrangements are reasonable, and "accurate information is deemed competent without the requirement of the lawyer to make further inquiry or analysis."[258]

If approved, the new comment would clarify the State Bar of Georgia's stance on limited-scope representation while maintaining competence through the use of remote lawyering.

C. A Lawyer's Reasonable Efforts

Although a lawyer's duty of confidentiality and duty to safeguard client property are distinct concepts, they are generally synonymous with protecting clients.[259] The comments to Georgia Rule 1.6 provide

255. Suarez, *supra* note 11, at 400–17; Platt, *supra* note 3, at 810; Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp., Formal Op. 2011-200, at 1–2 (2020).

256. *See* RULES TO SERVE SELF-REPRESENTED LITIGANTS, *supra* note 102; N.C. State Bar, Formal Op. 2005-10, at n.1 (2006).

257. *See* N.C. State Bar, Formal Op. 2005-10 (2006) (addressing concerns of virtual practice, including "providing competent representation given the limited client contact").

258. *See* RULES TO SERVE SELF-REPRESENTED LITIGANTS, *supra* note 102.

259. *See* Storey, *supra* note 116.

little guidance as to the reasonableness of technological safeguards and the reasonableness of a lawyer's expectation of privacy in a particular mode of communication with a client, and Georgia Rule 1.15 provides no guidance as to cybersecurity measures regarding payments, identity theft, and clients' funds.[260] Accordingly, the comments should clarify these ambiguities.

First, Comment 24 to Georgia Rule 1.6 provides little guidance as to the reasonableness of efforts to prevent unauthorized disclosures.[261] It focuses mostly on a cost-benefit approach to risk analysis and does not address what a lawyer's specific reasonable efforts entail when vulnerabilities are detected in the firm's infrastructure.[262] Therefore, the comment should be amended to also include the following reasonable efforts as interpreted by the FTC and the courts.

> Proposed Comment: A lawyer's reasonable efforts to protect a client's confidences and property also include prompt reaction to combat any substantial security risks, restricting access to sensitive information with strong passwords, and continual network monitoring.[263] A lawyer should implement internal controls to regularly update and patch systems, including maintaining an adequate firewall and an antivirus and antimalware software. Finally, a lawyer should safeguard all clients' payment data and sensitive data through encryption.[264]

By clarifying some of the specific measures that will help lawyers protect their clients, this comment will assist lawyers in having conversations with tech support to ensure all are meeting their ethical duties in big and small firms alike.

260. *See* GA. RULES OF PRO. CONDUCT r. 1.6 cmts. 24, 25 (STATE BAR OF GA. 2021); *id.* r. 1.15.
261. *Id.* r. 1.6 cmt. 24.
262. *See id.*
263. *See* FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 241, 258 tbl. (3d Cir. 2015).
264. *See id.* at 241; *In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2583, 2016 WL 2897520, at *1 (N.D. Ga. May 17, 2016); *In re* Arby's Rest. Grp. Inc. Litig., No. 17-CV-0514, 2018 WL 2128441, at *10 (N.D. Ga. Mar. 5, 2018).

D. Law Firm Management

The Georgia Rules require lawyers who maintain a managerial position at a firm to "make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Georgia Rules."[265] The duty of a lawyer's supervisory role also includes ensuring that "nonlawyers in the firm will act in a way compatible with the Georgia Rules."[266] The lawyer should take into account that these employees "do not have legal training and are not subject to professional discipline," unlike the lawyer.[267] Further, if the lawyer retains or directs technology vendors such as cloud providers, consultants, and other technology professionals outside of a firm, "a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer."[268]

Because of the important supervisory role that many lawyers play, the comments that accompany Georgia Rules 5.1 and 5.3 should be updated to reflect the duty of technological competence and clarify the ambiguity regarding "reasonable measures" undertaken by lawyers who are partners, managers, or supervisors in a firm. The comment below proposes the following additions to clarify a lawyer's duty.

> Proposed Comment: Lawyers who supervise other lawyers and nonlawyers must take reasonable measures to assure that the firm complies with a lawyer's duty of technological competence, including but not limited to a duty to train employees to handle confidential information, detect cyberattacks, and monitor the network, external data

265. GA. RULES OF PRO. CONDUCT r. 5.1 cmt. 2 (STATE BAR OF GA. 2021).
266. *Id.* r. 5.3 cmt. 2.
267. *Id.* r. 5.3 cmt. 1.
268. *Id.* r. 5.3 cmt. 4.

> sources, and outside vendors.[269] Lawyers must ensure that the firm has an incident response plan in place suited to the firm's needs.[270]

There are substantial infrastructural differences between small and large firms, and to account for these differences, the following checklists from *The ABA Cybersecurity Handbook* provide advice tailored to firm size to support supervisory lawyers in undertaking reasonable measures.[271]

1. Big Law

Cybersecurity measures are important to clients and the firm's reputation.[272] "Continual [p]rocess [i]mprovements" in a firm's cybersecurity management plan are necessary as technologies evolve.[273] To start, checklists can help with developing procedures to assess and mitigate cybersecurity threats, ensuring such procedures contain necessary elements.[274] If a breach occurs, large law firms should consider relationships with "crisis management, public relations, and . . . forensic firms."[275] Large firms should utilize the following checklist to assess and manage risks.

269. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 4–5 (2018); ABA Comm. on Ethics & Pro. Resp., Formal Op. 08-451, at 2 (2008); *see* Ige & Esther, *supra* note 232 (explaining the need for practical training).

270. ABA Comm. on Ethics & Pro. Resp., Formal Op. 483, at 6 (2018); Raul & Hanley, *supra* note 218.

271. *See* Raul & Hanley, *supra* note 218, at 204–05; Theodore L. Banks, *Cybersecurity for the Little Guys*, *in* ABA CYBERSECURITY HANDBOOK, *supra* note 23, at 207, 217 tbl.

272. Raul & Hanley, *supra* note 218, at 197.

273. *Id.* at 203.

274. *See id.* at 204–05.

275. *Id.* at 204.

Table 1. Cybersecurity Checklist for Big Law[276]

Number	Item	Description
(1)	Cybersecurity Risk Profile	Create a risk profile that details the "current data and device controls in place, the nature of data and information accessed by the firm, ethical obligations, and other relevant factors."[277]
(2)	Evaluation of Data	Account for "client-specific data security considerations . . . that may require additional steps" because of the sensitive nature of the data and/or additional laws and regulations that govern the data.[278]
(3)	Information Security and Data Governance Committee	Charge the committee to "obtain a basic understanding of the NIST Cybersecurity Framework that approaches cyber risks."[279]
(4)	Chief Information Security Officer (CIO)	Appoint or hire a CIO to manage the cybersecurity risks, train staff, and stay current on technologies.[280]
(5)	Information Security Program	Create and "implement a standardized, auditable risk-based information security program addressing cybersecurity."[281]
(6)	Data Security Requirements	Software, cloud, and other vendor contracts should have "stringent requirements for data security."[282]
(7)	Incident Response Plan	Involve employees in escalating cyber events as well as developing protocols to provide notice to "clients, government authorities, or individuals."[283]

276. *Id.* at 204–05.
277. *Id.*
278. Raul & Hanley, *supra* note 218, at 204.
279. *Id.* The NIST Framework for Improving Critical Infrastructure Cybersecurity consists of the following core functions: "identify, protect, detect, respond, and recover." *Id.* at 198 n.39.
280. *Id.* at 205.
281. *Id.*
282. *Id.*
283. *Id.*

(8)	Internet and Device Security	"Develop controls on Internet access and the use of personal devices by members and employees of the firm."[284]
(9)	Training	Educate lawyers and nonlawyer staff on the firm's technologies and cybersecurity.[285]
(10)	Routine Audits	Routinely audit "security risks and vulnerabilities."[286]

2. Small Firms and Solo Practitioners

Cybersecurity is not just for big firms; small firms and solo practitioners are not immune to security threats either.[287] Much like big firms, small firms need to be positioned to pass potential clients' security audits.[288] All firms can take measures to "maintain a secure and reliable computer system."[289] To progress towards this goal, small firms should consult the below checklist below which has been reproduced from *The ABA Cybersecurity Handbook*.

284. Raul & Hanley, *supra* note 218, at 205.
285. *Id.*
286. *Id.*
287. Banks, *supra* note 271, at 207.
288. *Id.* at 208–09.
289. *Id.* at 216.

Table 2. Cybersecurity Checklist[290]

Item	Description	Date Completed
Inventory	Hardware, software, outside services, security for each, consequences of failure	
Data Types	Specific legal requirements, client requirements	
Outside Contractor	On call to provide support for routine and nonroutine needs	
Security Review	Cloud service security examined; procedures for log-in security	
Firm Cybersecurity Policy	Rules for data protection; training of employees; physical security; password protection; wireless security; need-to-know access to firm data; antivirus software	
Sensitive Information	Limit on devices used to access firm/client data	
Encryption	All devices used to access or store firm/client data; document password protocol	
Backup	Cloud backup systems; local backup devices; security	
Records Management	Creation, maintenance, and security of records; limitations on access	
Cyber Insurance	Policy obtained; policy understood	
Website Security	Protect against hacking	
Mobile Access	Rules understood; security in place; VPN	

290. *Id.* at 217 tbl. This table is a reproduction of the table provided in *The ABA Cybersecurity Handbook*.

These lists are not exhaustive, and lawyers must also remember that all firms can learn from each other in their use of technology and implementation of cybersecurity measures.[291] The ABA's checklists provide a starting place for communication about cybersecurity planning as part of a lawyer's duty of technological competence within the firm.

CONCLUSION

The legal profession's dependency on technology did not develop overnight with the onset of the COVID-19 pandemic.[292] The pandemic did, however, increase lawyers' reliance on technologies to facilitate remote work, communication, research, and advocacy.[293] The legal profession's increasing dependence on technology necessitates that lawyers be technologically competent.[294] Georgia lawyers need further guidance to understand their ethical duty concerning the technologies that they rely on to provide services, communicate, store, and transmit information.

Technological competence requires understanding the "benefits and risks associated with relevant technology," which includes a "fact-based analysis" to employ "reasonable efforts" with respect to the duty of confidentiality.[295] Although technology solutions are not one-size-fits-all, and a variety of checklists can be adapted for specific needs, reasonable methods to protect clients' information can be implemented, including firewalls, strong passwords, VPNs, and encryption, as seen in FTC consent decrees and case history.[296] By explicitly acknowledging the duty of technological competence exists and by providing further guidance to practitioners who are seeking to

291. *See* Bell, *supra* note 206.
292. *See* MOLITERNO, *supra* note 18, at 208–10.
293. Platt, *supra* note 3; McParland, *supra* note 4.
294. *See generally* Walters, *supra* note 5 (discussing the rise of AI in the legal profession and competence); McGinnis & Pearce, *supra* note 5 (discussing the rise of machine learning in the legal profession and competence).
295. *See* sources cited *supra* note 5.
296. Mills & Allende, *supra* note 188; *see Data Security*, *supra* note 205.

understand their ethical obligations, the State Bar of Georgia will better position Georgia's lawyers to advocate for and protect their clients.