# REGULATION OF THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE TOOLS IN THE DELIVERY OF LEGAL SERVICES: VERIFICATION AND ACCOUNTABILITY

Carol A. Needham*

## ABSTRACT

Use of generative artificial intelligence ("generative AI") by those delivering legal services presents challenges including preservation of confidentiality, verification, and accountability. State-level and federal agency guidance in the United States often requires lawyers using generative AI to ensure that the way the platform, system, or tool is handling and transmitting their prompts and other inputs does not compromise the confidentiality of information gained during representation of a client. It is virtually impossible, however, for a lawyer to obtain the access to the technology provider's proprietary information about the algorithms and operation of the LLMs that would be needed to comply with that level of diligence regarding the operation of the technology. Even guidance which requires only that lawyers take "reasonable steps" does not specify what attainable level of diligence in a lawyer's investigation of a vendor's cybersecurity practices, handling of user inputs, and data privacy commitments for the generative AI the lawyer is using will be regarded as sufficiently rigorous.

In response to this issue, this Article explains why regulators are better positioned than lawyers to assess cybersecurity and to conduct investigations of the operations of generative AI products. Working with non-profit organizations or consultants with technical expertise, regulators can accomplish the desired level of assessment of the security of data input when generative AI is used in providing legal services. Additionally, this

* Emanuel Myers Professor of Law, Saint Louis University School of Law. The author would like to thank Peter DiCola, Barbara Glesner Fines, Marsha Griggs, Peter Joy, Wendy Muchman, Ellen Murphy, David Orozco, David Siegel, and Lindsey Simon for their ideas and comments on earlier drafts, as well as Stephanie Haley for outstanding work on the manuscript and Lynn Hartke for invaluable research assistance.

Article highlights how the current lack of a comprehensive set of federal regulatory requirements addressing the operation of generative AI contributes to the difficulty of performing adequate assessment of generative AI platforms, systems, and tools. Recognizing the limitations of the current guidance for attorneys practicing in the United States, this Article proposes a course of action addressing data confidentiality concerns while placing the burden of due diligence on those best positioned to adequately investigate—those who regulate the delivery of legal services.

## INTRODUCTION

Generative artificial intelligence (generative AI) is a powerful technology whose operation remains somewhat mysterious to many lawyers. After discussing key aspects of the legal profession's attempts to delineate the risks and benefits of using generative AI in the delivery of legal services in the United States, this Article highlights a crucial problem. Much of the emerging guidance requires lawyers to investigate details about the operation of a generative AI platform, system, or tool which cannot be confirmed without access to proprietary information. This information is, understandably, closely guarded by the technology companies whose platforms and generative AI tools the lawyers are using. The technical details underpinning generative AI platforms available for use by lawyers and law firms are widely discussed,[1] but full knowledge of the platform processes remains elusive. And, of course, the rapid pace at which technology is developing[2] can easily change the landscape. This makes it

1. *See generally* Mark L. Shope, *Lawyer and Judicial Competency in the Era of Artificial Intelligence: Ethical Requirements for Documenting Datasets and Machine Learning Models*, 34 GEO J. LEGAL ETHICS 191 (2021); W. Bradley Wendel, *The Promise and Limitations of Artificial Intelligence in the Practice of Law*, 72 OKLA. L. REV. 21 (2019); Peter K. Yu, *Artificial Intelligence, the Law-Machine Interface, and Fair Use Automation*, 72 ALA. L. REV. 187 (2020); James M. Cooper, *Are 'Friends' Electric?: A Comparativist Approach to Guidelines for the Development and Implementation of Artificial Intelligence in the People's Republic of China and the United States of America*, 42 B.U. INT'L L.J. 119 (2024); Austin G. Miller, Note, *Can a Light Bulb Turn on in the Mind of a Computer?—A Primer to the Issue of Whether AI Computers Are Capable of Conception*, 99 U. DET. MERCY L. REV. 95 (2021); Giovanni De Gregorio, *The Normative Power of Artificial Intelligence*, 30 IND. J. GLOB. LEGAL STUD. 55 (2023); David T. Laton, *Manhattan_Project.exe: A Nuclear Option for the Digital Age*, 25 CATH. U. J. L. & TECH. 94 (2016); Jan L. Jacobowitz & Justin Ortiz, *Happy Birthday Siri! Dialing in Legal Ethics for Artificial Intelligence, Smartphones, and Real Time Lawyers*, 4 TEX. A&M J. PROP. L. 407 (2018).

2. *See, e.g.*, Robin Feldman & Kara Stein, *AI Governance in the Financial Industry*, 27 STAN.

difficult to propose a description of the platforms, systems, and tools which will remain accurate as technological developments occur.

Generally, however, the term generative AI refers to algorithms that can be utilized to perform tasks such as making decisions based on data and to create new content, which can include text, video, images, or audio. Machine learning involves the use of algorithms to learn from a body of data and to adapt and make changes based on experience. It is broadly accurate to say that generative AI uses large language models (LLMs), which are machine-learning neural networks involving multiple neural network layers trained on enormous data sets. Generative AI is able to generate new content reflecting mathematical predictions of sequences[3] based on the data on which the provider's LLM was trained.[4] For purposes of this discussion, it may also be useful to include the definition of AI articulated in the October 30, 2023 Executive Order signed by United States President Biden.[5] This definition has been adopted by others addressing the use of the technology in the delivery of legal services: "The term 'artificial intelligence' or 'AI' has the meaning set forth in 15 U.S.C. § 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual

J.L. BUS. & FIN. 94, 132 (2022); Matthew R. Gaske, *Regulation Priorities for Artificial Intelligence Foundational Models*, 26 VAND. J. ENT. & TECH. L. 1, 16–17 (2023); ABA Comm. on Ethics and Pro. Resp., Formal Op. 512 (2024).

3. *See, e.g.*, MINN. STATE BAR ASS'N WORKING GRP. ON AI, IMPLICATIONS OF LARGE LANGUAGE MODELS (LLMS) ON THE UNAUTHORIZED PRACTICE OF LAW (UPL) AND ACCESS TO JUSTICE 4 (2024) [hereinafter Minn. SBA Working Group on AI Report] (after converting text to a string of numbers, AI tools use statistics and mathematics to predict and suggest the next set of numbers which is then displayed to the user as text).

4. *See, e.g.*, Michael F. Romano et al., *Large Language Models in Neurology Research and Future Practice*, 130 NEUROLOGY 1058, 1059 (2023), https://pmc.ncbi.nlm.nih.gov/articles/PMC10752640/ [https://perma.cc/JBR9-ALAW]; Karthick Panner Selvam et al., *Can LLMs Enhance Performance Prediction for Deep Learning Models?*, ICML 2024 WORKSHOP WANT (2024), https://openreview.net/pdf?id=bpS4vaOg7q [https://perma.cc/6HKG-FPZD] (accepted to Workshop on Advancing Neural Network Training at International Conference on Machine Learning); Muhammad Usman Hadi et al., *Large Language Models: A Comprehensive Survey of its Applications, Challenges, Limitations, and Future Prospects*, TECHRXIV, Nov. 16, 2023, at 1–2, https://d197for5662m48.cloudfront.net/documents/publicationstatus/181139/preprint_pdf/edf41a1f2a93aadb235a3c3aff2dcf08.pdf [https://perma.cc/4MUQ-7Z43].

5. Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 30, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/ [perma.cc/CFW2-DJV5] [hereinafter Exec. Order No. 14110].

environments."[6] As further stated in the statute: "Artificial intelligence systems use machine- and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action."[7] Although Executive Order No. 14110 was rescinded on January 20, 2025,[8] and additional action related to AI is anticipated in an Executive Order signed on January 23, 2025,[9] to date there has been no change in the statutory definition of artificial intelligence.

Generative AI involves a type of AI which has been designed to summarize, understand, predict, and generate new content. Data is entered into an LLM and the output (or response to a prompt) if it's in the form of text is what the LLM's algorithm predicts as the next word or phrase. The Report and Recommendations of the New York State Bar Association Task Force on Artificial Intelligence contains a description of the development of the technology that is particularly useful for lawyers without a computer science background in its sections titled: Evolution of AI and Generative AI,[10] and Benefits and Risks of AI and Generative AI Use.[11] An important thing to keep in mind about generative AI is that the mathematical relationship is what drives the response from the tool. As noted in the June 2024 report of the Minnesota State Bar Association Working Group on AI, AI tools "convert text to a string of numbers (vector embeddings) and rely on statistics and math to 'predict' the next set of numbers which are then displayed as text."[12] Prompts or queries posed by a user are not typically stored as discrete documents within the platform or tool.[13]

The way the AI platforms and tools are utilized and the nuances of the

6. *Id.* § 3(b) (quoting 15 U.S.C. § 9401(3)).

7. 15 U.S.C. § 9401(3).

8. Exec. Order No. 14148, 90 Fed. Reg. 8237 (Jan. 20, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/ [https://perma.cc/Q9JX-5M9Q] (revocation of Executive Order No. 14110 along with seventy-seven other orders and presidential memorandums).

9. Exec. Order No. 14179, 90 Fed. Reg. 8741 (Jan. 23, 2025), https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriersto-american-leadership-in-artificial-intelligence [https://perma.cc/7QK7-CJHW].

10. TASK FORCE ON ARTIFICIAL INTELLIGENCE, N.Y. STATE BAR ASS'N, REPORT AND RECOMMENDATIONS TO NYSBA HOUSE OF DELEGATES 11–18 (2024).

11. *Id.* at 19–28.

12. Minn. SBA Working Group on AI Report, *supra* note 3, at 4.

13. *Id.* Although this may technically be the case, the ability of later users to shape their use of the platforms and tools so as to elicit specific data complicates the statement a bit.

prompts entered by users can affect the outputs received from the platforms. Providers reassure users that data on which generative AI has been trained ordinarily does not emerge as chunks in which the original source is identifiable. The way in which the generative AI platforms are handling and interacting with data differs from the way data was stored in searchable databases that lawyers have long used, such as those offered by LexisNexis, Westlaw, or Bloomberg. At the same time, it is also true that a user entering refined prompts can elicit responses from a generative AI tool or platform which convey information about specific inputs. In response to the prompt "animated sponge wearing pants," for example, AI image generators responded with copyrighted images of the cartoon character SpongeBob SquarePants.[14] The New York Times[15] and other newspapers[16] have sued providers of generative AI alleging that when prompted by users, the platform reproduced the newspapers' copyrighted material "verbatim or nearly verbatim."[17] The originators of the news stories understandably focus their pleadings on the argument that their copyright was violated.[18] All lawyers, however, would be well-advised to closely follow the developments in these lawsuits, particularly in the discovery phase of the litigation. The specific datasets and the particular iteration of the AI tools whose use gave rise to the litigation may not be those utilized by individuals providing legal services. However, the ability of the plaintiffs to elicit published news stories and other copyrighted material in the responses provided by the generative AI tools used must be taken into account by lawyers and by those regulating the delivery of legal services. If the

14. Stuart A. Thompson, *We Asked A.I. to Create the Joker. It Generated a Copyrighted Image*., N.Y. TIMES (Jan. 25, 2024), https://www.nytimes.com/interactive/2024/01/25/business/ai-image-generators-openai-microsoft-midjourney-copyright.html [https://perma.cc/R95P-U37C]; *see also* Maria Nava, *This Week in AI News: Taylor Swift Deepfake, Take 2 and Midjourney Images*, FRANKFURT KURNIT KLEIN + SELZ (Jan. 27, 2024, 18:14), https://technologylaw.fkks.com/post/102iyb9/this-week-in-ai-news-taylor-swift-deepfake-take-2-and-midjourney-images [https://perma.cc/C2LH-K4GX].

15. Bobby Allyn, *'New York Times' Sues ChatGPT Creator OpenAI, Microsoft, for Copyright Infringement*, NPR (Dec. 27, 2023, 1:47 PM), https://www.npr.org/2023/12/27/1221821750/new-york-times-sues-chatgpt-openai-microsoft-for-copyright-infringement [https://perma.cc/3TGG-3A8J].

16. *See, e.g.*, Blake Brittain, *OpenAI Hit with New Lawsuits from News Outlets over AI Training*, REUTERS (Feb. 28, 2024, 1:13 PM), https://www.reuters.com/legal/litigation/openai-hit-with-new-lawsuits-news-outlets-over-ai-training-2024-02-28/ [https://perma.cc/5FUK-7ZNU].

17. *Id.*; *see also* Complaint at 2–3, 65, N.Y. Times Co. v. Microsoft Corp., No. 1:23-cv-11195 (S.D.N.Y. Dec. 27, 2023).

18. Complaint at 16–22, 47–48, 60–65, N.Y. Times Co. v. Microsoft Corp., No. 1:23-cv-11195 (S.D.N.Y. Dec. 27, 2023).

plaintiffs' assertions are substantiated, we must acknowledge that motivated users who use the correct series of prompts—including competitors and opposing parties—might be able to elicit responses that reveal material from prompts and data input by a lawyer who had never intended the material to be revealed outside the attorney-client relationship. This has obvious and far-reaching implications for use of the tools by lawyers.

Part I of this Article discusses the emerging state-level guidance in the United States addressing the use of generative AI in the delivery of legal services. Part II focuses on guidance issued by the U.S. Patent and Trademark Office (USPTO) concerning proper use of generative AI by lawyers practicing before that federal agency. Compared to the existing state-level opinions and guidance, the USPTO guidance contains a much more detailed discussion of national security considerations and the impact of secrecy orders and export control regulations. However, the USPTO does not also specify what level of diligence in a lawyer's investigation of cybersecurity practices, data privacy policies, and other key terms of use for a generative AI platform they are utilizing will be regarded as sufficiently rigorous. Part III proposes that a significant portion of any necessary investigation into the operation of generative AI tools be conducted by regulators and affiliates who have the deep technical expertise and access needed to audit and assess the risks and adequacy of safeguards involved in the operation of the models. Further, these regulators and experts are well-positioned to analyze the security of the data input by lawyers as they use generative AI tools that tech companies are offering for use by those delivering legal services. Part IV of the article assesses the implications of the contrast between the elaborated regulatory structure within which financial institutions operate and the current level of regulation of the tech sector in the United States.

Finally, Part V discusses the differing degrees of alignment of interests between lawyers and tech companies in various use cases. When entering into an agreement for services such as cloud storage for a lawyer's practice, both parties to the contract have a strong interest in maintaining a high level of security for the client data being stored. When it comes to contracts involving generative AI, in contrast, the interests of the lawyer and the tech provider diverge. While lawyers want the same high level of security for any information related to the representation of their clients, the company providing the technology has a strong interest in developing and refining

their generative AI models and platforms. The potential gains from utilizing lawyers' prompts to train the LLMs may be difficult for a company to resist, even when doing so runs afoul of the terms of the contract between the lawyer and the tech company. In summary, this Article provides a snapshot of an evolving landscape and proposes elements necessary for a more effective regulatory response. This response is critical as generative AI platforms and tools targeted to the legal services market continue to develop and the risks and benefits associated with using generative AI in connection with delivering legal services become more widely understood.

## I. GUIDANCE AND REPORTS ADDRESSING THE USE OF GENERATIVE AI IN DELIVERING LEGAL SERVICES

In a number of jurisdictions in the United States, legal ethics counsel, working groups, and bar association committees have prepared reports and guidance addressing issues related to the use of generative AI in providing legal services. These include California,[19] District of Columbia,[20] Florida,[21] Kentucky,[22] Michigan,[23] Minnesota,[24] New York,[25] Pennsylvania,[26] Virginia,[27] and West Virginia.[28] Task forces and similar groups in additional

19. State Bar of Cal. Standing Comm. on Pro. Resp. & Conduct, *Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law* (Nov. 2023), https://www.calbar.ca.gov/Portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf [https://perma.cc/V6P6-JNCC] [hereinafter Cal. State Bar Practical Guidance for the Use of Generative AI].

20. D.C. Bar Legal Ethics Comm., Op. 388 (2024) [hereinafter D.C. Bar Op. 388].

21. Fla. Bar, Ethics Op. 24-1 (2024).

22. Ky. Bar Ass'n, Op. E-457 (2024).

23. State Bar of Mich., Op. JI-155 (2023).

24. Minn. SBA Working Group on AI Report, *supra* note 3, at 36–37.

25. N.Y. City Bar Ass'n Comm. on Pro. Ethics, Formal Op. 2024-5 (2024), https://www.nycbar.org/reports/formal-opinion-2024-5-generative-ai-in-the-practice-of-law/ [https://perma.cc/BX5P-GVKM]; TASK FORCE ON ARTIFICIAL INTELLIGENCE, *supra* note 10.

26. Pa. Bar Ass'n Comm. on Legal Ethics & Pro. Resp. & Phila. Bar Ass'n Pro. Guidance Comm., Formal Op. 2024-200 (2024) [hereinafter Pa. & Phila. Formal Op. 2024-200], https://www.pabar.org/Members/catalogs/Ethics_Opinions/Formal/Joint_Formal_Opinion_2024-200.pdf [https://perma.cc/A3DU-73QF].

27. *Legal Ethics*, VA. STATE BAR, https://vsb.org/Site/Site/lawyers/ethics.aspx [https://perma.cc/UHR8-NWTG].

28. W. Va. Jud. Investigation Comm'n, Advisory Op. 2023-22 (2023), https://www.courtswv.gov/sites/default/pubfilesmnt/2023-11/JIC%20Advisory%20Opinion%202023-22_Redacted.pdf [https://perma.cc/L5NA-UWFV]; W. Va. Law. Disciplinary Bd., Draft Op. 24-01 (2024), https://files.constantcontact.com/75edd16b001/db6ae758-78c8-41e3-93aa-cd57c1caeb03.pdf [https://perma.cc/P3HY-KXU3].

jurisdictions, including Texas,[29] are still at work. Advisory committees to state supreme courts, state bar committees, and other entities in jurisdictions including Missouri,[30] New Jersey,[31] North Carolina,[32] and Texas[33] have issued preliminary guidance, informal opinions, or proposed ethics opinions guiding generative AI use by those delivering legal services. Understandably, many of the entities issuing these documents acknowledge that their positions are subject to review and revision. Reports and opinions in Minnesota,[34] New Jersey,[35] New York,[36] and Texas,[37] for example, anticipate continuing refinement as developments occur. This is absolutely appropriate. Developments both in the technology itself, and shifts in the norms that are established in connection with the use of the technology, make such review particularly important in this area.

It is fine to state that, as a matter of competence, attorneys must

29. *See generally* TASKFORCE FOR RESPONSIBLE AI IN THE L., STATE BAR OF TEX., INTERIM REPORT TO THE STATE BAR OF TEXAS BOARD OF DIRECTORS (2023), https://www.texasbar.com/AM/Template.cfm?Section=Meeting_Agendas_and_Minutes&Template=/CM/ContentDisplay.cfm&ContentID=62597 [https://perma.cc/ZHR4-8HZ7].

30. Off. of Legal Ethics Couns. & Advisory Comm. of the Sup. Ct. of Mo., Informal Op. 2024-11 (2024), https://mo-legal-ethics.org/informal-opinion/2024-11/ [https://perma.cc/DGB2-B8UF].

31. *See generally* TASK FORCE ON ARTIFICIAL INTELLIGENCE AND THE L., N.J. STATE BAR ASS'N, REPORT, REQUESTS, RECOMMENDATIONS, AND FINDINGS (2024), https://njsba.com/wp-content/uploads/2024/05/NJSBA-TASK-FORCE-ON-AI-AND-THE-LAW-REPORT-final.pdf [https://perma.cc/M9BJ-BL9V] [hereinafter NJSB Task Force on AI and the Law Report].

32. *Proposed Opinions*, N.C. STATE BAR (July 18, 2024), https://www.ncbar.gov/for-lawyers/ethics/proposed-opinions/ [https://perma.cc/68QF-U6JF] (under Council Actions, see Proposed 2024 Formal Ethics Op. 1: Use of Artificial Intelligence in a Law Practice).

33. *See* State Bar of Tex. Pro. Ethics Comm., Proposed Op. (PO-2024-6) (Nov. 19, 2024) (proposed Texas opinion by Texas State Bar Professional Ethics Committee).

34. Minn. SBA Working Group on AI Report, *supra* note 3, at 36–37 (recommending inter alia establishment of an AI Standing Committee to further explore potential use cases and creation of a legal sandbox to foster innovation).

35. NJSB Task Force on AI and the Law Report, *supra* note 31, at 6 ("This report acknowledges the ever-evolving nature of AI and offers initial guidance, rather than definitive policies. Subsequent tools and recommendations will be provided as the technology progresses, with a continued emphasis on practicality.").

36. TASK FORCE ON ARTIFICIAL INTELLIGENCE, *supra* note 10, at 53 (recommending that the New York State Bar Association convene a group to consider periodic updates to the state's generative AI guidance, "As the impacts [of AI technology] are continual, so should the updates to these guidelines be as well."); N.Y. City Bar Ass'n Comm. on Pro. Ethics, Formal Op. 2024-5, at 1 ("This summary of currently available tools will likely soon be outdated because of the rapid evolution of Generative AI. . . . We expect that this advice will be updated and supplemented in years to come to cover issues not yet anticipated.").

37. TASKFORCE FOR RESPONSIBLE AI IN THE LAW, *supra* note 29, at 1 ("The emphasis is on continued research, collaboration, and thoughtful development in this rapidly evolving landscape. Regulation and technology will both continue to evolve over the course of this work.").

understand the limitations of generative AI. District of Columbia Ethics Opinion 388 articulates a point made by virtually every ethics opinion on the topic when it says: "[L]awyers who rely on [a particular] technology should have a reasonable and current understanding of how to use the technology with due regard for its potential dangers and limitations."[38] This is appropriate and unobjectionable. It is also reasonable for a court to require that attorneys confirm the validity of the legal authorities on which they rely in briefs filed with the court. Federal courts, including the Second Circuit,[39] the District Court for the Middle District of Florida,[40] the District Court for the Southern District of New York,[41] and the District Court for the Eastern District of California,[42] have uniformly held that attorneys are responsible for confirming the existence and validity of authorities cited in their briefs before they file them.

However, opinions issued by some courts, as well as by various entities in the United States providing guidance for attorneys' use of generative AI, go farther and contain requirements that are beyond the abilities of lawyers to meet. Rejecting a report generated by ChatGPT which had been filed in support of the reasonableness of a law firm's motion for attorney's fees, a federal judge in New York faulted the lawyers who had filed the report for not identifying "the inputs on which Chat GPT relied" in its response to the lawyers' queries; and for not determining whether any of these inputs were imaginary.[43] Confirming the validity of judicial opinions included in briefs can certainly be required as a matter of competent exercise of professional judgment. However, an attorney should not be required to investigate and identify the inputs on which a generative AI tool has been trained or has used in responding to an attorney's prompts.

38. D.C. Bar Op. 388, *supra* note 20 (the requirement is anchored in District of Columbia's rule articulating the duty of competence).

39. Park v. Kim, 91 F.4th 610, 615 (2d Cir. 2024).

40. *In re* Neusom, No. 2:24-MC-2-JES, 2024 WL 1013974, at *2 (M.D. Fla. Mar. 8, 2024) (suspending attorney for one year and adopting the Grievance Committee finding detailed in *In re* Neusom, No. 2:23-cv-00503-JLB-NPM, 2024 WL 982508 (M.D. Fla. Jan. 11, 2024)).

41. Mata v. Avianca, Inc., 678 F. Supp. 3d 443, 464–65 (S.D.N.Y. 2023).

42. *See* U.S. v. Hayes, No. 2:24-cr-0208-DJC, 2025 WL 235531, at *9 (E.D. Cal. Jan. 17, 2025) (imposing $1,500 sanction for including a non-existent case citation and quotation in a motion and reply and then repeatedly misrepresenting to the Court that the non-existent case was real, noting that "[c]iting nonexistent case law or misrepresenting the holding of a case is making a false statement to the court. It does not matter if generative AI told you so." (quoting Maura R. Grossman et al., *Is Disclosure and Certification of the Use of Generative AI Really Necessary?*, 107 JUDICATURE 68, 75 (2023))).

43. J.G. v. New York City Dep't of Educ., 719 F. Supp. 3d 293, 308 (S.D.N.Y. 2024).

The New Jersey Preliminary Guidelines require that the lawyer "ensure the security" of an AI system before entering any non-public client information.[44] In the Report of the New Jersey State Bar Task Force on Artificial Intelligence (AI) and the Law, lawyers are required to evaluate the generative AI providers' privacy protocols and cybersecurity safeguards.[45] California State Bar guidance on the point states: "A lawyer who intends to use confidential information in a generative AI product should ensure that the provider does not share inputted information with third parties or utilize the information for its own use in any manner, including to train or improve its product."[46] Similarly, an opinion jointly issued by committees of the Pennsylvania Bar Association and the Philadelphia Bar Association provides that, "Lawyers must safeguard information relating to the representation of a client and ensure that AI systems handling confidential data (1) adhere to strict confidentiality measures, and (2) confidential data will not be shared with other clients or others not protected by the attorney-client privilege."[47] The opinion goes on to state, "Lawyers must ensure that the data used to train AI models is accurate, unbiased, and ethically sourced to prevent perpetuating biases or inaccuracies in AI-generated content."[48]

The D.C. Bar opinion[49] is a good example of the lacunae in even a thoughtfully drafted opinion. It requires both that lawyers "ensure" that the generative AI tool[50] they are using "has implemented adequate security

44. "A lawyer is responsible to ensure the security of an AI system before entering any non-public client information." N.J. SUP. CT. COMM. ON ARTIFICIAL INTELLIGENCE AND THE CTS., PRELIMINARY GUIDELINES ON NEW JERSEY LAWYERS' USE OF ARTIFICIAL INTELLIGENCE 1, 5 (2024) [hereinafter NEW JERSEY PRELIMINARY GUIDELINES].

45. "Evaluating [AI] vendors' data collection and ownership standards, privacy protocols and cybersecurity safeguards is essential for ensuring client confidentiality and regulatory compliance . . . It is important to assess the cybersecurity measures implemented by the vendor to maintain data integrity and avoid or minimize the risks posed by cyber threats." NJSB Task Force on AI and the Law Report, *supra* note 31, at 18.

46. Executive Summary, State Bar of California Standing Committee on Professional Responsibility and Conduct, Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law, at 2 (Nov. 16, 2023).

47. Pa. & Phila. Formal Op. 2024-200, *supra* note 26, at 15.

48. *Id.*

49. The opinion states: "Lawyers must . . . ensure that AI systems handling confidential data (1) adhere to strict confidentiality measures, and (2) confidential data will not be shared with other clients or others not protected by the attorney-client privilege." It further requires: "Lawyers must ensure that the data used to train AI models is accurate, unbiased, and ethically sourced to prevent perpetuating biases or inaccuracies in AI-generated content." *Id.*

50. The terms "gen AI," "GAI," and "generative AI" are used interchangeably throughout the various authorities' discussion of the technology.

safeguards and controls to ensure confidentiality and protect against unauthorized access and use of client information," as well as whether it uses a narrow data-set with out of date or inaccurate information and is thus problematic.[51] To protect client confidences and secrets, the opinion suggests that lawyers should ask two questions:

1. Will information I provide to the GAI be visible to the GAI provider or other strangers to the attorney-client relationship?
2. Will my interactions with the GAI affect answers that later users of the GAI will get in a way that could reveal information I provided to the GAI?[52]

In addition, the D.C. Bar Opinion notes that business users who pay to use a generative AI product may be able to better negotiate more user-protective terms than are available to users of a "free" service (that the provider makes available for the provider's own marketing and product development purposes).[53] For example, the contract might include a clause specifying a "zero data retention policy" in which the generative AI provider promises to retain neither the inputs nor the outputs of the generative AI's interaction with a particular user.[54] This does not go far enough. It is not possible for the average attorney to verify the answers they receive to those questions from the generative AI providers. Attorneys and other customers are locked out of the proprietary processes that the generative AI providers are using. Even if the contract a lawyer signs with the provider does contain better, more user-protective terms (like a zero data retention policy), the attorney has no way of ascertaining whether the company is abiding by the terms of the agreement. The D.C. Bar Opinion also states that, "Attorneys who would provide client confidences and secrets to a GAI product should ensure that product has implemented adequate security safeguards and controls to ensure confidentiality and protect against unauthorized access and use of client information."[55]

51. D.C. Bar Op. 388, *supra* note 20.
52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*

The opinion, like those of other jurisdictions,[56] does not specify what will be considered to be a sufficient due diligence process. These opinions and guidance should do one of two things: either specify the steps that an attorney can undertake that will be regarded as enough to meet the requirement that the attorney must evaluate the adequacy of the company's security safeguards and controls; or point the attorney to a continuously updated resource that clarifies the steps and methodology that is required. It must be noted that a handful of jurisdictions, including Michigan,[57] Missouri,[58] and Virginia,[59] mandate only that a lawyer take "reasonable steps" to assess the adequacy of the generative AI provider's security measures. And, in a proposed opinion, North Carolina says both that a lawyer must simply "make reasonable efforts,"[60] while at the same time must also "take steps to ensure" that confidential client information remains secure.[61] Following a nuanced discussion of the risk that using a generative

56. Those jurisdictions include Kentucky, Michigan, Missouri, New Jersey, New York, North Carolina, and Pennsylvania. *See generally*, *supra* notes 22–23, 25–26, 30–32 (absence of guidance for what constitutes sufficient due diligence).

57. "If a lawyer elects to utilize an AI tool and decides to input confidential information and has received client consent, the lawyer must take reasonable steps to determine whether the AI provider has adequate security measures [sic] in place to maintain and protect client confidences and secrets." *Artificial Intelligence for Attorneys—Frequently Asked Questions*, STATE BAR OF MICH., https://www.michbar.org/opinions/ethics/AIFAQs [https://perma.cc/DZZ5-TKW2] (last updated May 2024).

58. Off. of Legal Ethics Couns. & Advisory Comm. of the Sup. Ct. of Mo., Informal Op. 2024-11 (2024), https://mo-legal-ethics.org/informal-opinion/2024-11/ [https://perma.cc/DGB2-B8UF] ("In considering the use of a generative AI platform or service, lawyers are required to make reasonable efforts to safeguard client confidential information in accordance with Rule 4-1.6(c) and Lawyer should consider the guidance of Comment [15] as to how client confidential information will be safeguarded."). But note that the informal opinion also states that the "Lawyer needs to carefully assess any generative AI platforms or services that will be used by Law Firm to ensure confidentiality of client information is maintained." That assessment should include consideration of factors including: "the terms and conditions of using a generative AI platform or service to understand the security of the information being inputted, how that information is being used by the platform or service, and what data sources the platform or service is using to produce responses to prompts or queries." *Id.* (citing Informal Op. 2018-04; Informal Op. 2021-12).

59. *Legal Ethics*, *supra* note 27 ("[L]awyers must make reasonable efforts to assess . . . security and evaluate whether and under what circumstances confidential information will be protected from disclosure to third parties.") (on website, under Legal Ethics Topical Information, then Guidance on Generative Artificial Intelligence, then Confidentiality).

60. N.C. State Bar, 2024 Formal Ethics Op. 1 (2024) (Use of Artificial Intelligence in a Law Practice) ("A lawyer utilizing an outside third-party company's AI program or service must make reasonable efforts to ensure that the program or service used is compatible with the lawyer's responsibilities under the Rules of Professional Conduct pursuant to Rule 5.3.").

61. *Id.* ("A lawyer that inputs confidential client information into an AI tool must take steps to

AI tool could result in improper disclosure of client information (even when the tool is used exclusively by lawyers within the same law firm), the American Bar Association (ABA) Standing Committee on Ethics and Professional Responsibility embraces a risk-based approach.[62] In its discussion of confidentiality and informed consent, the opinion ultimately says that lawyers should understand the terms of use, privacy policy, and related contractual terms and policies of any generative AI tool they use.[63] This is quite different from requiring that lawyers ascertain precisely how the tool is operating.

However, lawyers are more commonly required to go further, and to "ensure" that the generative AI systems and tools they are using have adequate security measures in place. Similar requirements are specified for lawyers practicing in jurisdictions including the District of Columbia,[64] Florida,[65] New Jersey,[66] New York,[67] and Pennsylvania.[68] State opinions commonly point to attorneys' duties of confidentiality and competence as the reason that they mandate attorneys' investigation of the generative AI platforms, systems, and tools. The opinion of the Kentucky Bar Association is a good example on this point. The opinion first sets out the requirement,

---

ensure the information remains secure and protected from unauthorized access or inadvertent disclosure per Rule 1.6(c).").

62. ABA Comm. on Ethics & Pro. Resp., Formal Op. 512 (2024) (discussing the use of generative artificial intelligence tools).

63. *Id.* at 7 ("As a baseline, all lawyers should read and understand the Terms of Use, privacy policy, and related contractual terms and policies of any GAI tool they use to learn who has access to the information that the lawyer inputs into the tool or consult with a colleague or external expert who has read and analyzed those terms and policies.").

64. *See supra* note 20 and accompanying text.

65. *See* Terrence P. McAvoy & Michael Zhang, *Florida Bar Advisory Opinion 24-1 Gives Green Light to Generative AI Use by Lawyers—With Four Ethical Caveats*, HINSHAW L. (Feb. 5, 2024), https://www.hinshawlaw.com/newsroom-updates-lfp-florida-bar-advisory-opinion-generative-ai-lawyers-ethical-caveats.html [https://perma.cc/A95L-BRNE].

66. NEW JERSEY PRELIMINARY GUIDELINES, *supra* note 44, at 5 ("When evaluating AI tools and services, it is essential to identify and document how data, especially client data, is transmitted, used, and stored by the AI to ensure its confidentiality. This information should guide the assessment of whether a particular AI tool is suitable for its intended use."). Essentially, a lawyer is responsible to ensure the security of an AI system before entering any non-public client information.

67. When using AI or generative AI tools, attorneys "must take precautions to protect sensitive client data and ensure that no Tool compromises confidentiality. . . . Further, you should periodically monitor the Tool provider to learn about any changes that might compromise confidential information." TASK FORCE ON ARTIFICIAL INTELLIGENCE, *supra* note 10, at 58.

68. "Lawyers must safeguard information relating to the representation of a client and ensure that AI systems handling confidential data [] adhere to strict confidentiality measures." Pa. & Phila. Formal Op. 2024-200, *supra* note 26, at 2.

"To prevent or reduce . . . risk of disclosure, the attorney must *ensure* that the use and the retention of confidential client information by an AI provider is secure and avoids confidentiality risks."[69] In further explanation it notes, "There are GAI systems that promise that the provider will not send a client's information off-site, or host or share third party content. If that promise is confirmed in writing, then it may be allowable to input the client's confidential information with that provider."[70] The idea that a written promise from the provider would be sufficient, of course, is in conflict with the idea that the attorney is responsible for ensuring the security protocols of the AI provider. The Kentucky opinion then circles back and declares that even with written confirmation from the company providing a generative AI system, "it still may be difficult, or even impossible to determine whether client information has been kept confidential."[71] The opinion concludes that "once the [client] information has been disclosed it has not yet been judicially determined whether sharing information with an AI program would render that information discoverable, and/or result in waiving claims of attorney-client privilege."[72]

Going forward, entities issuing opinions can realistically mandate that lawyers make "reasonable efforts" or take "reasonable steps" to explore the security measures and use of data protocols which the tech provider has in place for a generative AI platform or tool a lawyer is considering using. Language in the contract between the lawyer and the tech company providing generative AI, at a minimum, should require zero data retention and prohibit any provider use of prompts or data input by the lawyer in any way without prior disclosure to and approval by the lawyer. Specifying the elements of a sufficient due diligence process, as detailed earlier herein,[73] would be an even better approach. When designating these requirements, it is important that lawyers are only required to take actions which are within the lawyers' control. When lawyers are unable to obtain access to crucial information regarding the LLMs tech providers are offering for their use, they cannot confirm or ensure that the operation of the generative AI tools or platforms complies with the terms of their contract with the tech provider.

69. Ky. Bar Ass'n, Ethics Op. KBA E-457, at 9 (2024) (emphasis added).
70. Ky. Bar Ass'n, Ethics Op. KBA E-457, at 9 (2024).
71. *Id.*
72. *Id.*
73. *See supra* notes 57–58 and accompanying text.

We cannot require a person to take an action which they do not have the capacity to perform.

## II. FEDERAL GUIDANCE

Additional areas of concern have been highlighted by federal agencies. The United States Patent and Trademark Office's (USPTO) guidance for persons practicing before the USPTO, for example, highlights national security considerations[74] and the impact on patentability issues specific to the USPTO.[75] The office also highlights more commonly discussed confidentiality and conflict of interest concerns.[76] Those practicing before the office are required to "ensure" that the confidentiality of client data is maintained.[77] The USPTO guidance also declares that "before using . . . AI tools, it is imperative for practitioners to understand an AI tool's terms of use, privacy policies, and *cybersecurity practices*."[78] As external users, of course, it may be difficult for lawyers and other practitioners to obtain sufficient information from the generative AI provider regarding the operation of the AI tool to assess the cybersecurity practices of the tech company providing the tool. There is no mention in the guidance of what level of diligence would be sufficient. The USPTO guidance also points out that disclosures of client information by a generative AI tool can implicate export control, foreign filing licenses, the patentability of the client's idea,

74. Guidance on Use of Artificial Intelligence-Based Tools in Practice Before the United States Patent and Trademark Office, 89 Fed. Reg. 25609, 25609 (Apr. 11, 2024).

75. The guidance first acknowledges: "Use of AI in practice before the USPTO can result in the inadvertent disclosure of client sensitive or confidential information, including highly sensitive technical information, to third parties." It then lists some examples of situations in which the disclosure can occur including "when aspects of an invention are input into AI systems to perform prior art searches or generate drafts of specification, claims, or responses to [USPTO] actions." If an AI system retains user-entered information, the guidance notes that it can be utilized "in a variety of ways by the owner of the AI system including using the data to further train its AI models or providing the data to third parties in breach of practitioners' confidentiality obligations to their clients . . ." Then the USPTO guidance warns, "If confidential information is used to train AI, that confidential information or some parts of it may filter into outputs from the AI system provided to others." *Id.* at 25617.

76. *See id.* at 25614–25617; 37 C.F.R. §§ 11.106, 11.107–11.109 (2024).

77. Guidance on Use of Artificial Intelligence-Based Tools in Practice Before the United States Patent and Trademark Office, 89 Fed. Reg. 25609-02, 25617 (Apr. 11, 2024) ("When practitioners rely on the services of a third party to develop a proprietary AI tool, store client data on third-party storage, or purchase a commercially available AI tool, practitioners *must be especially* vigilant to *ensure* that confidentiality of client data is maintained." (emphasis added)).

78. *Id.* (emphasis added).

and national security issues.[79] When generative AI tools use servers that are located outside the United States, data entered into the tools may be exported outside the United States, which may violate: national security regulations, export control regulations, or secrecy orders.[80] Even if the servers used by a generative AI tool are located within the United States, certain activities related to the use of AI systems hosted by these servers by non-U.S. persons may be deemed an export subject to these regulations.[81] Further, the USPTO guidance also points out that the companies developing or maintaining the generative AI platforms or tools may themselves suffer data breaches, which would further subject user data to disclosure risks.[82]

After detailing the potential harms, the USPTO, like the state ethics opinions, places the responsibility for investigation on the attorney and warns that attorneys using the platforms or tools should be "especially vigilant."[83] As with the state guidance and ethics opinions, this leaves open the question of what actions by attorneys will be considered to be sufficiently vigilant. How will the attorney be able to actually confirm that confidentiality of client data is maintained? Is it enough that the contract between the attorney and the provider of the generative AI tool specifies that the data will be protected? What steps is an attorney required to take to accomplish the anticipated level of due diligence and investigation? Ultimately, it is not feasible for the customers to *ensure* that the company providing the generative AI tool is complying with the terms of the contract. Lawyers would be realistically able to comply with a requirement that they must exercise "reasonable vigilance" or use "best efforts" to evaluate whether the companies providing generative AI are complying with their contractual obligations. But requiring a lawyer to "ascertain" or "ensure" matters beyond the lawyer's control saddles the lawyer with a requirement that she cannot meet.

79. *Id.*

80. *See, e.g.*, 37 C.F.R. § 5.11 (2024) (requirements for filing or exporting an application for an invention made in the United States, or technical data related to that invention to a foreign country); Scope of Foreign Filing Licenses, 73 Fed. Reg. 42781-01 (July 23, 2008).

81. Guidance on Use of Artificial Intelligence-Based Tools in Practice Before the United States Patent and Trademark Office, 89 Fed. Reg. 25609-02, 25617 (Apr. 11, 2024).

82. *Id.*

83. *Id.* ("Therefore, before using these AI tools, it is imperative for practitioners to understand an AI tool's terms of use, privacy policies, and cybersecurity practices.").

## III. REGULATORS ARE WELL-POSITIONED TO ACT

Since individual lawyers are unable to effectively hold the companies providing generative AI accountable, an authority with the ability to do so should step forward. In light of the seriousness of the potential harm, it is imperative that regulators, the entities responsible for articulating the standards applicable to those providing legal services, take an active role in assessing generative AI platforms, systems, and tools used by lawyers in representing clients. As used in this Article, the term "regulator" includes the entity in each state—typically the jurisdiction's highest court or its designee—which authorizes individuals to provide legal services. If the court chooses to do so, it may delegate some of the actions described herein to an advisory committee or to a specially constituted entity.

Regulators must articulate the standards that platforms, systems, and tools offered by generative AI providers must meet before they can be used by lawyers in that jurisdiction when providing legal services. The standards must be stated with enough specificity to be enforceable. If legislatures enacted effective statutory penalties for dissemination of confidential information, it might be possible to adopt some or all the statutory standards. But currently, in the United States at least, technology is developing faster than sufficiently protective statutes are being enacted. Although beyond the scope of this Article, developments elsewhere—including the European Union (EU) Artificial Intelligence Act,[84] the EU's AI Innovation Package,[85] and Coordinated Plan on AI,[86] along with the contrasting principles-based approach in England and Wales[87]—are likely to provide a useful

84. Regulation of the European Parliament and of the Council 2024/1689, 2024 O.J. (L 1689) 1 (EU) [hereinafter EU AI Act].

85. Press Release, Eur. Comm'n, Commission Launches AI Innovation Package to Support Artificial Intelligence Startups and SMEs IP/24/383 (Jan. 24, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_383 [https://perma.cc/9PZ3-4SEB].

86. *Coordinated Plan on Artificial Intelligence 2021 Review*, EUR. COMM'N (Apr. 21, 2023), http://digital-strategy.ec.europa.eu/library/coordinated-plan-artificial-intelligence-2021-review [https://perma.cc/3P4K-A4D2].

87. In England and Wales, the United Kingdom's principles-based AI Policy Paper supports sector-led regulation English regulation. *See generally* DEP'T FOR SCI., INNOVATION & TECH. & OFF. FOR ARTIFICIAL INTELLIGENCE, POLICY PAPER: A PRO-INNOVATION APPROACH TO AI REGULATION (2023) (United Kingdom government). Various reports and guidance were produced in response to the Department for Science, Innovation & Technology's request for the sector's strategic approach to AI. *See Risk Outlook Report: The Use of Artificial Intelligence in the Legal Market*, SOLICS. REGUL. AUTH. (Nov. 20, 2023), https://www.sra.org.uk/sra/research-publications/artificial-intelligence-legal-market/

comparative perspective when U.S. legislators do address these issues. In addition, regulators must also impose significant consequences on companies when the generative AI platforms or tools they provide to lawyers are found to fall short of the required standards. This can include striking a company from the list of approved providers, which would put the potentially lucrative market of legal services providers out of reach for those companies.

So, what requirements should be imposed on the vendors? As a condition of approving lawyers' use of a tool, the regulators should insist upon transparency and the ability to fully audit. That is, the regulator should have the on-going opportunity to conduct thorough technical reviews of the AI platforms and tools the company proposes to offer to those providing legal services. It is likely that, rather than hiring full-time employees to perform the reviews, the regulator will retain consultants—independent experts with sufficient technical knowledge and access—to ascertain whether the generative AI platform or tool does, in fact, operate as specified in the contract between the company and the lawyer. This utilization of experts on the technology is referenced by the ABA's Formal Opinion 512[88] and by some states, including New Jersey.[89] The New Jersey Task Force wrote, "When developing or implementing AI systems, collaboration with data privacy experts, cybersecurity professionals and/or AI professionals is highly recommended to ensure responsible integration and adherence to

[perma.cc/2CUT-EHGZ]; THE L. SOC'Y, LAW SOCIETY RESPONSE TO UK GOVERNMENT WHITE PAPER: *A PRO-INNOVATION APPROACH TO AI REGULATION* 1 (2023); THE INFO. TECH. PANEL, THE BAR COUNCIL, CONSIDERATIONS WHEN USING CHATGPT AND GENERATIVE ARTIFICIAL INTELLIGENCE SOFTWARE BASED ON LARGE LANGUAGE MODELS 5–7 (2024); E-mail from Richard Orpin, Interim Chief Exec., Legal Servs. Bd., to Michelle Donelan, Sec'y of State for Sci., Innovation & Tech. & Alex Chalk, Lord Chancellor and Sec'y of State for Just. (Apr. 29, 2024), https://legalservicesboard.org.uk/wp-content/uploads/2024/04/Legal-Services-Board-update-on-AI-approach-April-2024-pdf.pdf [perma.cc/Y44A-R2ZV] (response to the Department for Science, Innovation & Technology's Request for the Sector's Strategic Approach to AI).

88. ABA Comm. on Ethics & Pro. Resp., Formal Op. 512 (2024) ("Lawyers may need to consult with IT professionals or cyber security experts to fully understand these terms and policies as well as the manner in which GAI tools utilize information.").

89. TASK FORCE ON ARTIFICIAL INTELLIGENCE AND THE LAW, *supra* note 29, at 6 ("As technology evolves, and with cloud computing and AI becoming increasingly integral to legal practice, lawyers may lose additional control over data privacy and security. Consequently, some of the responsibility for protecting sensitive information may need to shift from law firms to their technology providers, potentially enhancing data protection as these providers are often better equipped to manage sophisticated privacy and cybersecurity challenges.").

ethical and legal standards."[90] It seems clear that involving advisors with deep technical expertise will be essential to understanding the operation of the generative AI platforms and tools.

These experts must be selected by the regulator and their work directed by the regulator, not the companies. It is important that, under this regime, all the work of ensuring that the vendor is appropriately handling the data associated with lawyers' use of the company's generative AI tool will be assessed by the regulators and their technical consultants, rather than by the individual lawyers. The regulator can strike from the list of eligible providers any company which is found to be handling data in a way that violates the terms of the contract between the company and the lawyers. It may be possible that one or more entities with the necessary technical expertise could perform reliable assessments that are useful to a number of jurisdictions. A voluntary process along the lines of that for Leadership in Energy and Environmental Design (LEED) certification or fair-trade coffee designation might also be considered. Those seeking the designation would first comply with the process overseen by experts, such as that run by the United States Green Building Council in the case of LEED certification. Then, after that voluntary process, attorneys and law firms could more confidently utilize generative AI platforms and tools provided by the vendors whose products had been assessed and found to be suitable for the legal services market. Coordination of the technical testing across jurisdictions could also be cost-effective. There is no need for every regulator to duplicate assessments that have already been performed by others.

If regulators are not yet prepared to take on the task of evaluating the operation of the generative AI platforms, there is another avenue. They can articulate the level of investigation which will satisfy the diligence requirement. It is crucial, of course, that the required level of diligence must be capable of being performed by lawyers who do not have specialized technical expertise and who do not have access to the proprietary workings of the models. It may take some time, and consultation with working groups including regulators, members of the bar, and those who can contribute based on their work with LLMs and other technical expertise, before the necessary standards can be articulated. In the meantime, it would be realistic

90. *Id.*

to require lawyers and law firms to insist upon language in their contracts with generative AI vendors that commits the vendors to requirements such as specified appropriate levels of data security, utilization of protocols in data transmission that meet articulated standards, and agreement not to retain lawyers' inputs or use them for training.

## IV. COMPARISON WITH REGULATION OF FINANCIAL INSTITUTIONS

If this proposal for action by regulators seems onerous, we can consider some comparisons with the regulators' involvement in specifying requirements which financial institutions have to meet before attorneys are allowed to open client trust accounts in those institutions. There has been plenty of innovation in the financial sector and many companies offer attractive rates and access for funds on deposit. Of course, not all the innovative participants in the market are allowed to hold attorneys' client trust accounts. There are some good reasons for that caution. The problems that accountholders experienced after the implosion of Synapse Financial Technologies (Synapse) are just one example of the potential dangers. In the "banking as a service" segment of the fintech industry, tens of thousands of account holders were locked out of their accounts when middleman Synapse collapsed.[91] Customer-facing startups that relied on Synapse to process transactions were unable to function when Synapse filed a petition in bankruptcy court.[92] Millions of dollars were suddenly tied up in a snarl of insufficient documentation and uncompleted transactions.[93] Months after Synapse filed a petition in bankruptcy, court-appointed Chapter 11 trustee Jelena McWilliams reported a shortfall between $65 million and $95 million.[94] Some of that money may eventually be available to the account

91. Hugh Son, *Savings App CEO Says 85,000 Accounts Locked in Fintech Meltdown: 'We Never Imagined a Scenario Like This'*, CNBC (June 1, 2024, 8:00 AM), http://www.cnbc.com/2024/06/01/synapse-bankruptcy-yotta-accounts-locked.html [https://perma.cc/JRA7-66DZ].

92. Teresa Xie, *How Safe is Your Money in a Fintech, Really?: QuickTake*, BLOOMBERG L. NEWS (Oct. 9, 2024, 3:58 PM), https://news.bloomberglaw.com/bankruptcy-law/how-safe-is-your-money-in-a-fintech-really-quicktake [perma.cc/2J5E-W4XA].

93. *See, e.g.*, Son, *supra* note 91 (noting Adam Moelis, the CEO of Yotta, reported that, "85,000 Yotta customers with a combined $112 million in savings have been locked out of their accounts.").

94. Chapter 11 Trustee's Fourth Status Report, *In re* Synapse Financial Techs., Inc., No. 1:24-bk-10646-MB, at 5–6 (Bankr. C.D. Cal. July 3, 2024) (describing reconciliation efforts and estimating the shortfall to be in the range of $65 to $96 million dollars).

holders,[95] but the claims process is likely to be far more onerous than any of the account holders anticipated when they deposited their funds. And, for a subset of accountholders, the outcome will be even worse—some of the shortfall may never be recovered.

Freed of the capital requirements and other regulations that banks must comply with, the innovative "banking as a service" startups had offered attractive rates and other apparent advantages as compared with traditional banks. When problems arose, however, Federal Deposit Insurance Corporation (FDIC) insurance was not available for fintech account holders when complete and accurate deposit account records were not available for funds deposited through non-bank companies.[96] Concerns about uninsured losses also arose in connection with the collapse of Silicon Valley Bank and the failure of Signature Bank in 2023.[97] It is notable that although uninsured depositors have, in the past, occasionally been made whole after the failure of an institution, the FDIC is not required to do so.[98] The good news for

95. Rob Copeland, *What Happens When Your Bank Isn't Really a Bank and Your Money Disappears?*, N.Y. TIMES (July 9, 2024), https://www.nytimes.com/2024/07/09/business/synapse-bankruptcy-fintech-fdic-insurance.html [https://perma.cc/3UN8-F74Z].

96. *See* Recordkeeping for Custodial Accounts, 89 Fed. Reg. 80135-01 (Oct. 2, 2024);

Martin J. Gruenberg, Chairman FDIC, Board Meeting Statement, Notice of Proposed Rule: Requirements for Custodial Deposit Accounts with Transactional Features and Prompt Payment of Deposit Insurance to Depositors (Sept. 17, 2024), https://www.fdic.gov/news/speeches/2024/notice-proposed-rule-requirements-custodial-deposit-accounts-transactional [https://perma.cc/D58J-2WTZ.

97. Martin J. Gruenberg, Chairman of FDIC, Speech at Florence School of Banking and Finance: Lessons Learned from the U.S. Regional Bank Failures of 2023 (May 17, 2024), https://www.fdic.gov/news/speeches/2024/lessons-learned-us-regional-bank-failures-2023 [https://perma.cc/8RKE-2JAE].

98. *See, e.g.*, *Banking with Third-Party Apps: What to Know About Fintech, Banking Relationships, and Deposit Insurance*, FDIC, https://www.fdic.gov/consumer-resource-center/2024-06/banking-third-party-apps [https://perma.cc/4BRW-JE23] (last updated May 31, 2024); *Deposit Insurance FAQs*, FDIC, https://www.fdic.gov/resources/deposit-insurance/faq#:~:text=If%20a%20depositor%20has%20uninsured,assets%20of%20a%20failed%20bank [https://perma.cc/Z8HH-54TV] (as the receiver for an insured bank, the FDIC will sell off the bank's assets and properly documented deposits above the insured amount can receive a portion of the sale proceeds); Adam Rust, *The Synapse Crisis Reveals the Urgent Need for Supervision of BaaS*, CONSUMER FED'N OF AM. (July 8, 2024), https://consumerfed.org/the-synapse-crisis-reveals-the-urgent-need-for-supervision-of-baas/ [https://perma.cc/NR75-T2Z2] (when funds are held in "for benefit of" (FBO) accounts, where ledgers are not kept that can verify end-user balances, FDIC insurance should not be available for those deposits); *see also* Letter from Consumer Federation of America & Americans for Financial Reform Education Fund, to the Office of the Comptroller of the Currency, Federal Reserve Board of Governors, & FDIC (Oct. 30, 2024) (in response to Request for Information on Bank Fintech Arrangements Involving Banking Products and Services Distributed to Consumers and Businesses – Docket No. OCC-2024-0014, Docket No. OP-1836, RIN 3064-ZA43), https://www.fdic.gov/federal-register-publications/consumer-federation-america-americans-financial-reform-education-fund [https://perma.cc/PA6X-NGA6]; FDIC Official Signs and Advertising Requirements, False Advertising, Misrepresentation of

lawyers' clients is that their funds are not often tied up for months or altogether gone due to a financial institution's insolvency. Because lawyers are fiduciaries, they have an obligation to safeguard client property.[99] Therefore, lawyers ensure that detailed records are maintained regarding the amount on deposit for each client and hold client funds in accounts opened in heavily regulated "banks,"[100] or "banking institutions,"[101] a term which includes savings banks and credit unions.[102] As a result of opening accounts directly with regulated banking institutions, their clients' funds are better protected.[103]

Jurisdictions in the United States commonly specify characteristics financial institutions must have before attorneys in the jurisdiction can open client trust accounts with them. California, for example, defines eligible

Insured Status, and Misuse of the FDIC's Name or Logo, 89 Fed. Reg. 3504, 3516 (Jan. 18, 2024) (amending 12 C.F.R. § 328).

99. All jurisdictions in the United States have adopted a rule regarding attorneys' duties related to the safekeeping of client property. Those which follow the ABA Model Rules express these duties in a comment. *See* MODEL RULES OF PRO. CONDUCT r. 1.15 cmt. 1 (AM. BAR ASS'N 2023) ("A lawyer should hold property of others with the care required of a professional fiduciary."). Other jurisdictions articulate this duty in the jurisdiction's rule itself. *See, e.g.*, N.Y. RULES OF PRO. CONDUCT r. 1.15(a) (2022) ("A lawyer in possession of any funds or other property belonging to another person, where such possession is incident to his or her practice of law, is a fiduciary, and must not misappropriate such funds or property or comingle such funds or property with his or her own.").

100. *See, e.g.*, CAL. BUS. & PRO. CODE § 6212 (West 2024) (explaining that lawyers must hold client funds in an interest-bearing bank account).

101. *See, e.g.*, 22 N.Y. JUD. LAW § 1200.0, r. 1.15(b)(1) (McKinney 2024) (explaining that New York's definition of a "banking institution" includes "a state or national bank, trust company, savings bank, savings and loan association or credit union").

102. The Federal Deposit Insurance Corporation (FDIC) provides insurance for qualifying fiduciary accounts. Insurance for accounts at credit unions is offered by the National Credit Union Administration (NCUA). *See Frequently Asked Questions About Share Insurance*, NAT'L. CREDIT UNION ADMIN., https://ncua.gov/consumers/share-insurance-coverage/frequently-asked-questions-about-share-insurance [https://perma.cc/8PTM-6U8G] (the National Credit Union Share Insurance Fund, administered by NCUA, insures funds held in accounts at most state-chartered credit unions as well as at all federal credit unions).

103. Lawyers are generally required to exercise prudence, taking steps a reasonable investor would take to safeguard the funds and guard against foreseeable risks. *See* Bazinet v. Kluge, 788 N.Y.S.2d 77, 78 (N.Y. App. Div. 2005); *Client Trust Accounts and Bank Stability Concerns*, STATE BAR OF CAL., https://www.calbar.ca.gov/Attorneys/Conduct-Discipline/Client-Trust-Accounting-IOLTA/Client-Trust-Accounts-and-Bank-Stability-Concerns [https://perma.cc/KH2Q-TTXF]; Marjorie E. Gross, *The Lawyer's Duties Regarding Deposit Insurance of Attorney Trust Accounts*, N.Y. STATE BAR ASS'N (Oct. 2, 2023), https://nysba.org/the-lawyers-duties-regarding-deposit-insurance-of-attorney-trust-accounts/ [https://perma.cc/XLC7-LWAF]; Ruth Smith, *What Lawyers Need to Know About Bank Failures and Trust Accounts*, FLA. BAR NEWS (Nov. 1, 2008), https://www.floridabar.org [https://perma.cc/677T-G5ZL].

institutions in § 6213(k) of the California Business and Professions Code.[104] In Illinois, under the state's Rule of Professional Conduct 1.15(b), lawyers are required to use an eligible financial institution for their client trust accounts.[105] Illinois Rule 1.15C(d) defines an eligible financial institution as a bank or savings bank insured by the FDIC, or a specific type of investment company registered with the SEC, which has agreed to notify the Attorney Regulation and Discipline Commission (ARDC) of any overdraft of a trust account and that offers Interest on Lawyer's Trust Accounts (IOLTA) accounts meeting the Illinois Rule 1.15C(b) requirements.[106] The Lawyers Trust Fund of Illinois maintains a list of financial institutions eligible to hold client trust accounts.[107] To qualify for FDIC "pass-through" insurance on deposits in fiduciary accounts, the account must be identified as a fiduciary account in the bank's account records and either the bank or the attorney must document the identity and ownership interest of each owner of the deposited funds.[108] Also note that in determining the insured amount for each owner, any other deposits the owner holds at the same bank which are in the same deposit insurance category will be added to their portion of the client trust account, with a $250,000 limit for the total insured amount for each deposit insurance category for that owner.[109] A lawyer would be vulnerable to claims they had acted improperly[110] if they ignored the obligation to safeguard client

104. An "eligible institution" is defined as either (1) a bank, savings and loan, or other financial institution regulated by a federal or state agency that pays interest or dividends on the IOLTA account and carries deposit insurance from an agency of the federal government or (2) any other type of financial institution authorized by the California Supreme Court. CAL. BUS. AND PROF. CODE § 6213(k) (West 2024).

105. ILL. SUP. CT. R. 1.15(b).

106. ILL. SUP. CT. R. 1.15C(d) (an "eligible financial institution" is a bank or a savings bank insured by the FDIC or an "open-end investment company registered with the Securities and Exchange Commission [SEC] that agrees to provide overdraft notification regarding any type of client trust account as provided in Rule 1.15B(e) and that, with respect to IOLTA accounts, offers IOLTA accounts within the requirements of Rule 1.1513(c)").

107. *See Eligible Financial Institutions*, LAW. TR. FUND OF ILL., https://ltf.org/lawyers/eligible-financial-institutions/ [https://perma.cc/KN2M-QD96].

108. *See Your Insured Deposits*, FDIC, https://www.fdic.gov/resources/deposit-insurance/brochures/insured-deposits [https://perma.cc/8FFK-QPS4]; *see also FDIC Coverage of IOLTA Deposits*, LAW. TR. FUND OF ILL., https://ltf.org/lawyers/fdic-coverage-of-iolta-deposits/ [https://perma.cc/73HG-LK3Y].

109. *Id.*

110. In addition to being subject to professional discipline, a lawyer might also face claims of malpractice or breach of fiduciary duty.

property and deposited client funds in accounts without proper recordkeeping in a less-regulated, under-capitalized non-bank entity.

The analogy with companies offering generative AI is not perfect, of course. Those regulating the delivery of legal services are not responsible for creating the regulatory safeguards for the banking sector. Legal services regulators simply utilize the requirements that financial institutions are already required to meet to be in compliance with the capitalization levels and other standards needed to be considered a bank, for example, under the existing banking regulations. A robust system of oversight, audit, and evaluation overseen in the United States by the Office of the Comptroller of the Currency[111] is relied upon by lawyers' regulators. We do not have to set up a parallel system among lawyers themselves to assess the safety of the financial institutions holding client trust accounts. In contrast, in the U.S., there is not yet a comprehensive set of regulatory requirements concerning the operation of their platforms, services, and tools that generative AI providers must comply with in order to remain in good standing. We have already seen some movement in this direction[112] and it is likely that additional requirements will be proposed as the industry matures. However, no comprehensive regulatory system has yet been imposed on generative AI providers. Therefore, the regulators of those delivering legal services cannot build upon a pre-existing external set of requirements.

Still, the fact remains that the regulators of legal services are far better positioned to set out minimum standards that companies providing generative AI platforms, services, and tools must comply with (and to ensure compliance with those standards) than is the average attorney. Individual lawyers and law firms typically do not have the ability to ensure that the companies providing generative AI in fact are complying with the contract terms and conditions of the agreements they sign with the lawyers.

111. *See Financial Institution Lists*, OFF. OF THE COMPTROLLER OF THE CURRENCY, https://www.occ.treas.gov/topics/charters-and-licensing/financial-institution-lists/index-financial-institution-lists.html [https://perma.cc/A5VN-VYBN]. Note that state banks are also supervised by state banking regulators.

112. Meaghan Tobin, *A.I. Pioneers Call for Protections Against 'Catastrophic Risks'*, N.Y. TIMES (Sept. 16, 2024), http://nytimes.com/2024/09/16/business/china-ai-safety.html [https://perma.cc/FH67-883L] (explaining that at a meeting convened by "Far.AI," a group including Yoshua Bengio, Andrew Yao, and Geoffrey Hinton, proposed that a system of global oversight should be developed to rein in the potentially cataclysmic risks that are posed by fast moving developments in AI).

## V. EFFECT OF DIFFERING INCENTIVES AND RISK-TAKING CORPORATE CULTURE

Some might argue that in using cloud storage and other services provided by external tech company vendors, lawyers are already taking the word of the technology companies regarding how confidential client information and other data input by a lawyer is handled by the tech company. After all, lawyers do not routinely get access to the code and other proprietary information the vendor is using to provide the storage. And lawyers using cloud storage products are not instructed to conduct additional investigation into the methods the vendor is using to protect the uploaded data and keep it safe from unauthorized access. Why not extend the same trust in the generative AI vendors' products? In a word: incentives. With regard to cloud storage, the incentives of the vendor and the lawyer are aligned. Both parties to the contract have strong incentives to keep the data that the lawyer is storing well-protected from unauthorized access. A vendor whose customers' data is exposed when the vendor's product is hacked (especially if it were repeatedly hacked) would have trouble staying in business. Customers would flee to a competing cloud storage provider. Lawyers have a similarly strong interest in the security of the data provided to the vendor. So, unless there is evidence otherwise, in the case of cloud storage it is reasonable for lawyers to assume that the vendor will honor the data security terms of the contract.

With generative AI, in contrast, the incentives diverge. The technology provider wants to develop and refine their generative AI platforms, services, and tools. There is an advantage for the provider in scooping up as much information as possible and using it to train the provider's products. Attorneys, on the other hand, want to keep control of the information and data that they are putting into the generative AI platforms, services, and tools. Revealing any of the information that is input, including the sequence of prompts, is potentially dangerous for the attorney and their client. The attorney does not want the information which they are entering to be utilized for any purpose or in any way other than that which is specified in the attorney's contract with the tech company providing the generative AI. With this divergence in incentives, it makes much less sense to assume that attorneys can simply rely on the tech company to scrupulously abide by the terms of the contract and forgo any utilization of the data entered by the

lawyer.

In addition, it would not be a stretch to observe that some of the companies developing generative AI platforms, services, and tools have a corporate culture that is far from risk-adverse and compliance-oriented. Accounts of a minimalist approach to honoring commitments which these companies have made are legion. As just one example, OpenAI pledged to the Biden Administration in 2023 that it would rigorously safety test new versions of its generative AI technology prior to its release to ensure that the technology would not cause catastrophic harm.[113] Just a few months later, in the spring of 2024, members of the OpenAI safety team responsible for performing those safety test reportedly were pressured to speed through the testing in just a few days so that the new version could be rolled out on the schedule announced by the company's top brass.[114] Company leaders, including CEO Sam Altman, have been accused of prioritizing commercial interests over public safety. As others have observed, this also raises questions about the United States federal government's reliance on self-policing by tech companies (through the White House pledge, as well as the now-rescinded October 2023 Executive Order on AI)[115] to protect the public from abuses of generative AI. While the European Union's Artificial Intelligence Act explicitly prioritizes the protection of fundamental human rights and ethical principles in AI development, with the goal of aligning AI applications with human values,[116] no similar explicit restraint is currently required under U.S. law. As Andrew Strait, formerly at Google Deep Mind and now Associate Director at the Ada Lovelace Institute in London, has

113. Melissa Heikkilä, *AI Companies Promised to Self-Regulate One Year Ago. What's Changed?*, MIT TECH. REV. (July 22, 2024), https://www.technologyreview.com/2024/07/22/1095193/ai-companies-promised-the-white-house-to-self-regulate-one-year-ago-whats-changed/ [https://perma.cc/3GPK-A75S]; Fact Sheet, White House, Biden-Harris Administration Secures Voluntary Commitments from Eight Additional Artificial Intelligence Companies to Manage the Risks Posed by AI (Sept. 12, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/09/12/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-eight-additional-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/ [perma.cc/6GVS-PWZS].

114. Pranshu Verma et al., *OpenAI Promised to Make Its AI Safe. Employees Say It 'Failed' Its First Test.*, WASH. POST (July 12, 2024, 7:00 AM), https://www.washingtonpost.com/technology/2024/07/12/openai-ai-safety-regulation-gpt4/ [https://perma.cc/32BB-KSTE] (the rigorous safety testing was supposed to ensure that the new version of OpenAI's technology "would not inflict damage—like teaching users to build bio-weapons or helping hackers develop new kinds of cyberattacks").

115. Exec. Order No. 14110, *supra* note 5.

116. *See* EU AI Act, *supra* note 84.

said: "We have no meaningful assurances that internal policies are being faithfully followed or supported by credible methods."[117] Note that prioritization of production schedules and profitability is certainly not limited to tech companies. Two recent examples commanded public attention. Wells Fargo's decade-long unlawful sales practices led to a $3 billion dollar settlement to resolve civil claims under the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA), potential criminal prosecution, and Security Exchange Commission (SEC) proceedings.[118] Additionally, Boeing had difficulties maintaining adequate quality control standards in the company's production of commercial airplanes.[119] It would therefore be prudent to establish stronger mechanisms for scrutinizing whether companies providing generative AI for lawyers' use in representing clients are, in fact, complying with the terms of their contracts with lawyers.

## CONCLUSION

Regulators, rather than individual attorneys, are in the best position to evaluate the operation of generative AI and to hold accountable companies providing generative AI platforms, services, and tools when data is not handled as contractually mandated. It is essential that those regulating the delivery of legal services in a jurisdiction clearly specify a realistic level of investigation which attorneys must do to ascertain whether the generative AI platforms, services, and tools offered for use by lawyers in fact do have appropriate safeguards. Individual attorneys have neither the access nor the expertise needed to fully evaluate how the data they input is being handled by the companies offering generative AI tools. They have no way of ensuring whether or not the technology vendors are complying with the provisions of their contracts with attorneys. Whether by hiring full-time

117. *Id.*

118. *See* Press Release, U.S. Dep't of Just., Wells Fargo Agrees to Pay $3 Billion to Resolve Criminal and Civil Investigations into Sales Practices Involving the Opening of Millions of Accounts Without Customer Authorization (Feb. 21, 2020), https://www.justice.gov/opa/pr/wells-fargo-agrees-pay-3-billion-resolve-criminal-and-civil-investigations-sales-practices [perma.cc/P92N-PZ5D].

119. *See, e.g.*, ORG. DESIGNATION AUTHORIZATION EXPERT REV. PANEL, SECTION 103 ORGANIZATION DESIGNATION AUTHORIZATIONS (ODA) FOR TRANSPORT AIRPLANES EXPERT PANEL REVIEW REPORT, 5, 36–37 (2024); Niraj Chokshi at al., *'Shortcuts Everywhere': How Boeing Favored Speed Over Quality*, N.Y. TIMES (Mar. 28, 2024), https://www.nytimes.com/2024/03/28/business/boeing-quality-problems-speed.html) [https://perma.cc/BEP6-HPE5].

employees with the necessary expertise, sharing costs across jurisdictions, or utilizing outside consultants, those regulating the delivery of legal services must establish systems for investigating tech companies' use of data input by attorneys and verifying that the companies are, in fact, abiding by the terms of their contracts with those delivering legal services.