NORTH CAROLINA JOURNAL of
LAW & TECHNOLOGY
Volume 27, Issue 3 2026

ARTICLE

ASSESSING RISK & PROTECTING PERSONAL DATA: AN EU APPROACH TO ARTIFICIAL INTELLIGENCE AS A MODEL FOR THE A.B.A.'S MODEL RULES

Jennifer J. Cook†

"There's a false narrative that [AI] governance slows things down. That's only when it's approached as a checkbox exercise. In reality, governance enables progress by creating clarity, trust, and accountability." — Gerald Kierce[1]

This Article is the first to examine the risk that attorneys' use of generative artificial intelligence ("AI") in legal practice poses to personal data and offer a comparison of the American Bar Association's ("A.B.A.") and European Union's ("EU") differing approaches to providing guardrails for the

© 2026 Jennifer J. Cook.

† Associate Professor of Law, University of North Dakota School of Law. With gratitude to my spouse, Drew, and my children, Lincoln and Samuel, for their unwavering support throughout the writing and publication process. This work is dedicated to my Dad, in loving memory, whose constant support of my career endeavors—especially the "good work" of practicing law to protect and advance civil rights—shaped my life beyond measure. And finally, with appreciation to my colleagues at the University of North Dakota School of Law and in the greater academic community for their encouragement and shared wisdom.

1. Diana Spehar, *2025 Gen AI Trends: Privacy, Adoption, and Compliance*, FORBES (May 31, 2025), https://www.forbes.com/sites/dianaspehar/2025/05/31/2025-gen-ai-trends-privacy-adoption-and-compliance/ [https://perma.cc/2YLX-DQDB] (quoting Trustable CEO Gerald Kierce).

use of AI technology. It is also the first to suggest the A.B.A. consider integrating the EU's risk-based AI classification system and data protection requirements into its Model Rules of Professional Conduct.

Table of Contents

I. Introduction 342
II. Generative Artificial Intelligence Poses Risks to Privacy & Personal Data 346
A. *Non-Consensual Data Collection, Retention, and Use* 347
B. *Data Leaks & Breaches and Unauthorized Data Sharing* 353
III. The A.B.A.'s Approach to Artificial intelligence 358
A. *The Duty of Confidentiality: Model Rule 1.6* 359
B. *Resolutions 112 and 604* 362
1. *Resolution 112* 362
2. *Resolution 604* 364
C. *Artificial Intelligence Task Force* 366
D. *Formal Ethics Opinion 512* 368
IV. The EU's Approach to Artificial Intelligence 371
A. *The Artificial Intelligence Act* 371
B. *General Data Protection Regulation* 375
V. An EU Model for the A.B.A.'s Model Rules of Professional Conduct 378
A. *Proposal: Create a Categorized AI Risk-Based Assessment Framework Modeled After the EU's Artificial Intelligence Act and General Data Protection Regulation* 379
B. *Counterarguments* 382
VI. Conclusion 383

I. Introduction

In the age of artificial intelligence ("AI"), professions across the globe are in the midst of rapid transformation as they grapple with the significant disruptions the introduction of generative AI has wrought throughout industries. For decades now, industries worldwide have integrated artificial intelligence technology into their business models

and services in varying degrees.[2] However, AI technologies have evolved by leaps and bounds since OpenAI's ChatGPT and other similar generative artificial intelligence platforms have appeared on the international stage.[3] Generative AI systems are an advanced type of artificial intelligence that utilizes machine learning—an AI system that is trained on large amounts of data to learn how to analyze data, identify patterns, and make predictions—to generate new and original content.[4] And with AI's generative evolution, the number of newcomers to AI adoption has significantly increased.[5] Moreover, these advancements in AI have dramatically upended how certain tasks within an industry are performed—bringing efficiency and effectiveness to the forefront.

While the use of AI and generative AI technology have undeniable benefits, efficiency, and effectiveness chief among them, those benefits do not come without risks. Experts warn about one such risk, the potential for significant job loss, unlike those seen before with other introductions of automated technologies, because "unlike past automation technologies, generative AI has the unique potential to impact all job sectors."[6] Predictions on how many jobs will be lost to

---

2. *See* Miriam Vogel, Michael Chertoff, Jim Wiley & Rebecca Kahn, *Is Your Use of AI Violating the Law? An Overview of the Current Legal Landscape*, 26 N.Y.U. J. LEGIS. & PUB. POL'Y 1029, 1031–33 (2023) ("[Artificial intelligence ("AI")] is not a singular technology, but rather a collection of them. . . . [T]ypes of AI technologies include speech recognition, deep learning, natural language generation, and machine learning"). "[Generative AI systems'] operation is predicated on machine learning processes inspired by neural networks in the human brain." Dr. Alvin Hoi-Chung Hung, *Analyzing the Primary and Attendant Risks of GAI-Based Natural Language Processing Models in Legal Research*, 39 SYRACUSE J. SCI. & TECH. LAW 15, 22 (2023–2024). Generative AI systems are a unique combination of types of AI technology, utilizing both natural language processing and machine learning. *Id.* at 23. This combination allows generative AI tools to understand human language, learn from vast training data sets whether in the form of text, audio, or images, and then generate original content in human language. *Id.*

3. Vogel, *supra* note 2, at 1033–34.

4. *Id.*

5. *Id.* at 1032 ("The adoption of AI has more than doubled in the last five years").

6. Ozge Demirci, Jonas Hanane & Xinrong Zhu, *Research: How Gen AI is Already Impacting the Labor Market*, HARV. BUS. REV. (Nov. 11, 2024),

footnote continued on next page

generative AI vary widely, with some business leaders estimating AI could "displace upward of [50%] of the white-collar workforce."[7] In contrast, a study conducted by Goldman Sachs indicates AI job displacement is initially limited, noting the "unemployment rate for AI-exposed occupations has now reconciled with the wider economy, refuting early fears of mass displacement."[8] Despite the looming yet ambiguously defined threat level to human-centered jobs, employers and employees already integrate or plan to integrate the use of generative AI tools into their business models and performance of fundamental work tasks.[9] More than 70% of Fortune 500 CEOs reported they anticipated adopting generative AI "within the next three years to improve employee productivity."[10]

Not one to be left behind, the legal profession has also begun to integrate the use of advanced AI and generative AI tools into the practice of law to complete core lawyering tasks like legal research and writing.[11] On the heels of the release of ChatGPT, both leading online legal research platforms, Thomson Reuter's Westlaw and RELX's

https://hbr.org/2024/11/research-how-gen-ai-is-already-impacting-the-labor-market [https://perma.cc/RGA9-NBU7] (commenting on the potential for significant economic disruption caused by generative AI adoption across industries and contrasting it to the limited job loss experienced by workers caused by Amazon's introduction of robotics to its warehouse operations in the early 2000s).

7. Nick Lichtenberg, *How Much is AI Really Replacing Jobs? Goldman Sachs Looks Under the Hood and Has 3 Takeaways to Defuse the Hype*, FORTUNE INTEL. (July 17, 2025, at 12: 35 ET), https://fortune.com/2025/07/17/will-ai-replace-jobs-labor-market-goldman-sachs-artificial-intelligence/ [https://perma.cc/5GXP-VH54].
8. *Id.*
9. *See generally*, Katharina Koerner, *Generative AI: Privacy and Tech Perspectives*, IAPP NEWS (Mar. 28, 2023), https://www.iapp.org/news/a/generative-ai-privacy-and-tech-perspectives/ [https://perma.cc/4GMD-VNU9] (noting "[generative AI's] global market size is expected to grow to over $200 billion by 2032").
10. Victor Dey, *Business Leaders Fret About Generative AI Despite Growing Enterprise Adoption: Study*, VENTUREBEAT (July 5, 2023), https://venturebeat.com/ai/business-leaders-fret-about-generative-ai-despite-growing-adoption [https://perma.cc/72ZB-QM5D].
11. Jennifer J. Cook & Denitsa Mavrova Heinrich, *AI-Ready Attorneys: Ethical Obligations and Privacy Considerations in the Age of Artificial Intelligence*, 72 U. KAN. L. REV. 313, 315 (2024).

LexisNexis, introduced generative AI platforms.[12] Westlaw's CoCounsel and LexisNexis's Protégé are capable of finding relevant legal authority, summarizing it for you, and then inserting the legal authority and client facts into a draft of a legal memo or client letter.[13]

With such intense focus on AI's rapid transformation of the economic and workforce landscape, industry leaders are keen to stay abreast of AI technological innovation to stay competitive in a global market, and workers are eager to develop AI skills to avoid becoming redundant in an "AI-fueled work environment."[14] But in the rush to adapt to advancements in AI, law firms, other industries, and workers must not ignore another, more imminent risk brought on by the newest AI revolution: The substantial risks the use of generative AI tools poses to the data privacy of individuals, organizations, and society.[15] The use of AI tools has always presented privacy risks. But with the advent of generative AI tools, those risks are more pronounced because of the tools' potent capabilities powered by copious amounts of data. Professionals who use generative AI tools to complete work tasks, particularly attorneys, must understand the privacy risks associated with the use of generative AI tools and take precautions to safeguard sensitive information while using those tools. Failure to do so can result in the exposure of client information that may violate an attorney's ethical duties.

Take the now-famous ChatGPT data breach, for example—the one that occurred just six months after its launch.[16] An internal bug in ChatGPT's system exposed the sensitive personal information of 1.2% of subscriber accounts, approximately 1.2 million users (exposed

---

12. *Id.*

13. *Id.* at 326.

14. Rachel Curry, *Recent Data Shows AI Job Losses Are Rising, but the Numbers Don't Tell the Full Story*, CNBC (Dec. 16, 2023, at 09:33 ET), https://www.cnbc.com/2023/12/16/ai-job-losses-are-rising-but-the-numbers-dont-tell-the-full-story.html [https://perma.cc/QAG2-SJ3S].

15. Koerner, *supra* note 9.

16. Eduard Kovacs, *ChatGPT Data Breach Confirmed as Security Firm Warns of Vulnerable Component Exploitation*, SECURITYWEEK (Mar. 28, 2023, at 08:59 ET),https://www.securityweek.com/chatgpt-data-breach-confirmed-as-security-firm-warns-of-vulnerable-component-exploitation/ [https://perma.cc/R9WN-9H3E (staff-uploaded, dark archive)].

information included: payment credit card information, payment/billing address, email address, and first and last names).[17] Portions of ChatGPT "users' chat history and the first message of a newly created conversation were [also] exposed in the data breach."[18] This privacy breach underscores the urgent need for strong privacy protocols where generative AI tools are used by attorneys as part of their law practice.

To help prepare attorneys to utilize generative AI tools ethically, this Article explores some of the privacy risks to personal data associated with the use of generative AI tools and proposes that the A.B.A. provide attorneys with more concrete guardrails for its use by incorporating EU-like privacy governance into its Model Rules of Professional Conduct. Part II examines the specific privacy risks and challenges posed by generative AI tools. Part III surveys the A.B.A.'s approach to governing attorneys' use of generative AI tools. Part IV discusses the EU's approach to governing artificial intelligence tools. And finally, Part V argues the A.B.A.'s guidance for attorneys on generative AI use falls short of globally accepted privacy and data protection standards and urges the A.B.A. to adopt an EU approach to generative AI regulation in its Model Rules of Professional Conduct.

II. Generative Artificial Intelligence Poses Risks to Privacy & Personal Data

The use of AI tools has always posed risks to privacy and personal data. However, the use of generative AI tools brings those existing risks into sharper focus and presents new privacy challenges that likely cannot be adequately addressed by existing U.S. data privacy protection frameworks, nor the A.B.A.'s Model Rules of Professional Conduct. Generative AI tools have inherent technical characteristics—power, speed, scope, sophistication, and inscrutability—that exacerbate long-recognized privacy risks

17. *Id.*; *see also Lessons Learned from the ChatGPT Data Breach*, Gaper, https://gaper.io/lessons-chatgpt-data-breach [https://perma.cc/WZ85-BJGU] (last visited Aug. 1, 2025).

18. Kovacs, *supra* note 16.

associated with the use of AI.[19] These characteristics, in combination with generative AI tools' need to consume large amounts of data to learn from and then generate new content, result in privacy harms such as: (1) non-consensual personal data collection, retention, and use; and (2) personal data leakage, breaches, and unauthorized third-party data sharing.[20] Other privacy harms beyond the two categories mentioned here exist; however, this Article focuses on these specific harms because they implicate globally accepted privacy principles, including data collection limitation and transparency, as well as attorneys' duty of confidentiality and other ethical duties.

A. Non-Consensual Data Collection, Retention, and Use

Generative AI tools require large amounts of digital data to function properly.[21] First, a generative AI system must be trained on large data sets so it learns how to replicate natural language, images, or audio to then create new content requested by its users' prompts.[22] Once the AI system learns from the initial training data set, it might also continue to learn or be trained on data retained from the information contained in a user's prompt to the AI system.[23] Initial

---

19. Elana Zeide, *Expanding the Paradigm: Generative Artificial Intelligence and U.S. Privacy Norms*, *in* CAMBRIDGE FORUM ON A.I.: LAW AND GOVERNANCE 1 (2025), https://www.cambridge.org/core/journals/cambridge-forum-on-ai-law-and-governance/article/expanding-the-paradigm-generative-artificial-intelligence-and-us-privacy-norms [https://perma.cc/RU5G-3PL3].

20. *Id.* at 2–3. Other privacy harms include data "re-identification, inferential profiling, synthetic media generation" and "exacerbation of algorithmic bias and discrimination; and decontextualized quantification." *Id.* at 2.

21. John Hillman, *Smart Regulation: Lessons from the Artificial Intelligence Act*, 37 EMORY INT'L L. REV. 775, 808 (2023).

22. Elysse Bell, *Generative AI: How it Works and Recent Transformative Developments*, INVESTOPEDIA, https://www.investopedia.com/generative-ai-7497939 [https://perma.cc/5LY2-PYR9] (last updated Jan. 7, 2025) ("Specifically, generative AI models are fed vast quantities of existing content to train the models to produce new content. They learn to identify underlying patterns in the data set based on a probability distribution and, when given a prompt, create similar patterns (or outputs based on these patterns).").

23. *See How Your Data Is Used to Improve Model Performance*, OPENAI, https//help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance [https://perma.cc/S2MH-UQHJ (staff-uploaded, dark archive)] (last visited Aug. 1, 2025).

training data is often scraped from publicly available data on the web.[24] While the scraped data can be stock photos or news articles, which clearly qualify as publicly available information, much of the training data can contain personally identifiable information like "individuals' names, addresses, and images published online under varying expectations of privacy."[25] Typically, an individual's personal data is given to a website with the individual's consent and after the individual is given notice about how their data will be used and shared.[26] However, the downstream use or data scraping of an individual's personal data from websites by generative AI companies, which occurs without specific consent from the individual web user, circumvents the notice and consent process.[27]

One such example of nonconsensual data collection involves Clearview AI, a facial recognition company, and its collection of data from social media platforms.[28] To train its AI systems, Clearview "scraped billions of digital images [from those platforms] without the knowledge or consent of the individuals depicted" in the images.[29] As one scholar noted, "AI systems like ChatGPT [or other generative AI tools] have been known to utilize personal data without explicit consent, thus blurring the lines between lawful and unlawful use of personal data."[30]

Alternatively, generative AI tools can collect and retain data without consent when a user provides the tools with information in a

---

24. Zeide, *supra* note 19, at 2–3. OpenAI's ChatGPT-4 trained on more than "45 terabytes of text data, including books, articles, and websites." *Id.* at 2.

25. *Id.*

26. *Id.* at 2–3; *see also* Cook & Mavrova Heinrich, *supra* note 11, at 347 ("In the United States, data privacy principles have long revolved around a 'notice and consent' model. This model is a form of market self-regulation and purports to provide individual consumers with the opportunity to approve whether they share data with a company . . . .").

27. Zeide, *supra* note 19, at 2–3; *see also* Michael P. Goodyear, *Circumscribing the Spider: Trademark Law and the Edge of Data Scraping*, 70 U. KAN. L. REV. 295, 298 (2021) (providing an overview of scrapping).

28. Zeide, *supra* note 19, at 3.

29. *Id.*

30. Cheng-chi (Kirin) Chang, *When AI Remembers Too Much: Reinventing the Right to Be Forgotten for the Generative Age*, 19 WASH. J.L. TECH. & ARTS 22, 33–34 (2023).

prompt to obtain new content (an image, text, or audio) from the generative AI tool. The information within the prompt may or may not be sensitive personal or business data. A recent report on generative AI data leakage indicated "8.5 percent of employee prompts to popular [generative AI tools] included sensitive data."[31] Sensitive personal or business data entered in a prompt to a generative AI tool risks exposure because that data might appear in a response provided by the generative AI tool at another time and to another user.[32] This can occur because the sensitive personal data is retained by the generative AI tool to further train and improve its system. ChatGPT's data use policy clearly indicates it retains information from users' prompts to further train and "improve [its] model['s] performance" unless an individual user opts out.[33]

From a law practice perspective, the leading legal research and writing generative AI tools from Thomson Reuters' Westlaw (CoCounsel) and RELX's LexisNexis (Protégé) had data collection, retention, and use policies that were challenging to understand and access when the products were first released in 2024 (CoCounsel) and 2025 (Protégé).[34] For instance, CoCounsel initially featured a hyperlink under its prompt box that indicated an attorney's "data [was] private

31. Evan Schuman, *Nearly 10% of Employee GenAI Prompts Include Sensitive Data*, CSO (Feb. 10, 2025), https://www.csoonline.com/article/3819710/nearly-10-of-employee-prompts-include-sensitive-data.html [https://perma.cc/5LJP-JSZD].

32. *See* Hoi-Chung Hung, *supra* note 1, at 38.

33. *See How Your Data Is Used to Improve Model* Performance, *supra* note 23.

34. From Capability to Confidence: How CoCounsel is Redefining Legal AI, Thomson Reuters (Mar. 31, 2026), https://legal.thomsonreuters.com/blog/from-capability-to-confidence-how-cocounsel-is-redefining-legal-ai/ [https://perma.cc/U7P6-JCG4] (discussing the integration of CoCounsel with Thomson Reuters content in early 2024); LexisNexis Introduces Protégé Personalized AI Assistant with Agentic AI, Making It Easier to Power Complex Legal Task Completion, LexisNexis (Jan. 27, 2025), https://www.lexisnexis.com/community/pressroom/b/news/posts/lexisnexis-introduces-protege-personalized-ai-assistant--making-it-easier-to-power-complex-legal-task-completion [https://perma.cc/U7P6-JCG4] (noting Protégé's release date).

and secure."[35] This hyperlink led to its AI Governance and Security Program white paper which provides, "[o]ur use of Large Language Modules (LLMs) is governed by Thomson Reuters' principles, frameworks, policies, and standards. We maintain governance policies and standards designed to minimize use of sensitive data in [training] AI models . . . ."[36] The "sensitive data minimization" phrase did not eliminate the possibility that a client's sensitive information provided in a prompt or uploaded in a document to CoCounsel will not be collected, retained, and used for the generative AI system's future training.

In early 2026, CoCounsel's "private and secure" language directly beneath its prompt box disappeared.[37] Now, a user must navigate to a sidebar and then select "legal information" from a multiple-item menu.[38] Once the "legal information" menu is selected, the user must then choose from seven menu items, which lead to information about: Terms of use, privacy, cookie settings, a cookie policy, a trust center, an AI usage policy, and a do not sell or share personal information opt-out.[39] Despite the array of information choices, the new multi-layered navigational approach makes it difficult to ascertain whether CoCounsel retains data from user prompts or documents and then trains its generative AI system with that data.[40] The AI usage policy only contemplates the user's responsibilities when interacting

35. CoCounsel Training: Welcome to CoCounsel, THOMSON REUTERS, https://training.thomsonreuters.com/media/Welcome%20to%20CoCounsel/1_et7h4jmd [https://perma.cc/FCS7-8SHZ] (last visited April 2, 2026). The training video captures CoCounsel's homepage and its prompt box as it appeared in fall 2025. *Id.*

36. *AI Governance and Security Program* 1, 4, THOMSON REUTERS (Mar. 2024), https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/information-security/thomson-reuters-ai-security-governance-whitepaper.pdf [https://perma.cc/M8QZ-HUA4].

37. CoCounsel Training: Welcome to CoCounsel, *supra* note 35; CoCounsel, THOMSON REUTERS, https://cocounsel.thomsonreuters.com/work/new-chat [https://perma.cc/Y4BY-VQ65] (last visited April 2, 2026).

38. CoCounsel, *supra* note 37.

39. *Id.*

40. *Id.*

with the tool, it does not limit or explain CoCounsel's data practices.[41] Further, the privacy menu provides that Westlaw, in general, "collect[s], use[s], disclose[s], and process[es] personal information . . ." such as: "user contributions and content" including "[p]ersonal information in content and communications uploaded, sent, shared, or inputted through our Services . . . including feedback you provide to us and the content of communications between you and us . . . including the content of your queries on our Services, such as artificial intelligence prompts . . . ."[42] Moreover, the privacy statement indicates personal information can be used "to operate, improve, or personalize . . . [s]ervices and [d]evelop new products, services, content, and other offerings."[43] Consequently, without an express statement otherwise, CoCounsel likely collects, retains, and uses information included in prompts or uploaded documents as part of the prompt to train its generative AI system.

Protégé's initial data collection, retention, and use practices were more unclear than CoCounsel. Protégé did not provide an attorney with a data security statement under its prompt box.[44] Rather, there were links to its privacy and processing policies.[45] The privacy policy expressly stated under its "Information We Collect" section and subsection "Data from Service Use:" "[T]he Service may automatically collect information about how you . . . interact with the Service, including: . . . the features you used, the settings you selected . . . [and] search terms you used . . . ."[46] The policy further provided under its "How We Use Your Information" section, "[W]e use your personal

---

41. *See* CoCounsel, *AI Usage Policy*, THOMSON REUTERS, https://www.thomsonreuters.com/content/dam/ewpm/documents/thomsonreuters/en/pdf/other/ai-usage-policy.pdf [https://perma.cc/GRN5-MDN6] (last visited Feb. 14, 2026).

42. CoCounsel, *Privacy Statement*, THOMSON REUTERS, https://www.thomsonreuters.com/en/privacy-statement [https://perma.cc/ZD6Z-29K9] (last visited Feb. 14, 2026).

43. *Id.*

44. *See Protégé in Lexis+AI: Guide for Law School Faculty*, RELX (Fall 2025) (on file with author). The guide captures images of the Protégé home page and its prompt box as it appeared in fall 2025.

45. *Id.*

46. *Privacy Policy*, LEXISNEXIS (Aug. 2025), https://www.lexisnexis.com/global/privacy/en/privacy-policy.page [https://perma.cc/XS5Z-J276].

information to . . . enhance and improve the Service and our other products, events, and services and to develop new products, services, and benefits . . . ."[47] The privacy policy failed to mention generative AI or AI model training, nor did it have a sensitive data minimization statement.[48] Like Westlaw's CoCounsel, this left open the possibility that LexisNexis's Protégé collected, retained, and utilized information an attorney provided in a prompt or an uploaded document to further "improve the Service," which likely included training its generative AI tool, Protégé.

However, in fall 2025, LexisNexis's Protégé provided its users with clearer information about its data collection, retention, and use practices.[49] Currently, Protégé assures its users that information provided in a prompt is not used to train its generative AI system.[50] Nor does it retain uploaded documents after an active Protégé conversation ends.[51] Additionally, users can delete conversations and documents from Protégé.[52] If users do not delete their chat history, Protégé will purge chats after ninety days.[53] Nonetheless, these same assurances do not extend to LexisNexis tools that are not powered by generative AI, such as its primary legal research query functions in Lexis+ AI, where the data collection and use policy outlined in the paragraph above likely still applies.

This initial lack of clarity from both CoCounsel and Protégé raises broad concerns about the potential downstream risks to personal data in an ever-evolving and shifting AI landscape—concerns that both users and vendors of generative AI tools must examine to avoid the consequences non-consensual data collection, retention, and use pose to data privacy. Although Protégé has taken steps to assure users that its generative AI tool mitigates data privacy risks, the ongoing

47. *Id.*

48. *Id.*

49. *Lexis+ AI Security Information*, RELX, https://engr2e.seismic.com/ls/b2c29b4e-6b5a-4789-a418-09cafaf53c98/0JHW3w0JV4DNkpmm [https://perma.cc/X8U3-5VFP] (last visited Feb. 14, 2026).

50. *Id.* at 7.

51. *Id.* at 2.

52. *Id.* at 1–2.

53. *Id.* at 1.

ambiguity and inaccessibility of CoCounsel's data collection, retention, and use practices continue to raise data privacy concerns.

B. Data Leaks & Breaches and Unauthorized Data Sharing

Non-consensual data collection, retention, and use can lead to several other privacy harms like data leaks, breaches, and unauthorized data sharing.[54] A data leak occurs when information is exposed "to parties that should not have access to it."[55] Regardless of whether the information is misused or abused, "the mere act of making data accessible to people who shouldn't be able to view it is data leakage."[56] One such example of data leakage is mentioned in the section above discussing non-consensual data collection, retention, and use. Recall that a generative AI tool that retains information its users provide in their prompts to train and improve its AI model could intentionally or unintentionally reveal sensitive personal data to another user when the tool generates a response to a user prompt.[57]

Whether information is non-consensually collected through web scraping or obtained through users' prompts, either method leaves the data vulnerable to leakage. In early 2025, cybersecurity experts focused on emerging generative AI threats found that "thousands of once-public GitHub repositories from some of the world's biggest companies" were appearing in "online generative AI chatbots like Microsoft Copilot long after the data [was] made private" despite only

---

54. *See* Zeide, *supra* note 19, at 3; *see also* Cook & Mavrova Heinrich, *supra* note 11, at 342–44 (discussing the inherent privacy risks to client data when law firms experience data breaches conducted by external hackers and external vendors leak or share client data).

55. Chris Tozzi, *How Bad is Generative AI Data Leakage and How Can You Stop It?*, INFORMA TECHTARGET (Dec. 19, 2024), https://www.techtarget.com/searchEnterpriseAI/answer/How-bad-is-generative-AI-data-leakage-and-how-can-you-stop-it [https://perma.cc/3NUK-FJ9L].

56. *Id.* (explaining that "data leaks can occur in a variety of technological contexts, not just those that involve GenAI. . . . A database that lacks proper access controls, or a cloud storage bucket that . . . is accidentally configure[ed] to be accessible to anyone on the internet, could also trigger unintended data exposure").

57. *Id.*

being "exposed to the internet, even for a moment."[58] Put simply, anyone browsing the internet might not find the now private data from the once public GitHub repositories; however, if a Copilot user asked the chatbot the "right question" in a prompt, the user could "get this data."[59] Some of the companies' exposed data included "intellectual property, sensitive corporate data, [and] access keys . . . ."[60] This specific example of data leakage illustrates the ability of any generative AI tool to scrape publicly available data on the web and use it to train and operate its system despite the fact that this practice directly results in data privacy harms.

While data leakage involves unintentional exposure of potentially sensitive data, the information that generative AI tools collect, use, and retain can also be intentionally exposed by malicious actors during a data breach. A data breach involves the unauthorized access to "sensitive or confidential information, including personal data (Social Security numbers, bank account numbers, healthcare data) and corporate data (customer records, intellectual property, financial information)" by unauthorized parties.[61] For example, a "ransomware attack that locks up a company's customer data and threatens to leak the stolen data unless the company pays a ransom" qualifies as a data breach.[62] An IBM report released in 2025 reveals that organizations that quickly implemented AI products into their business practices without accounting for and implementing strong cybersecurity and AI data governance practices are succumbing to data breaches.[63] The

58. Carly Page, *Thousands of Exposed GitHub Repositories, Now Private, Can Still Be Accessed Through Copilot*, TECHCRUNCH (Feb. 26, 2025, at 23:02 ET), https://techcrunch.com/2025/02/26/thousands-of-exposed-github-repositories-now-private-can-still-be-accessed-through-copilot/ [https://perma.cc/9GLX-LGJV].

59. *Id.*

60. *Id.* (revealing affected companies included "Amazon Web Services, Google, IBM, PayPal, Tencent, and Microsoft.").

61. Matthew Kosinski, *What Is a Data Breach?*, IBM, https://www.ibm.com/think/topics/data-breach [https://perma.cc/F5RG-EFB7] (last visited Aug. 1, 2025).

62. *Id.*

63. Dan Robinson, *Enterprises Neglect AI Security – and Attackers Have Noticed*, REGISTER (July 31, 2025), https://www.msn.com/en-us/money/other/enterprises

footnote continued on next page

report identified that "13 percent of [600 organizations] flagged a security incident involving an AI model or AI application . . . ."[64] Of those organizations that experienced a data breach, a third of those had sensitive data exposed to malicious actors.[65]

Importantly, the report noted a "majority of organizations that reported [a data breach] involving AI, said the source [of the breach] was a third-party vendor providing software as a service."[66] In response to the report, IBM's VP of Security cautioned, "[a]s AI becomes more deeply embedded across business operations, AI security must be treated as foundational. The cost of inaction isn't just financial, it's the loss of trust, transparency, and control . . . a gap between AI adoption and oversight already exists, and threat actors are starting to exploit it."[67]

The risk to personal data associated with the use of generative AI tools is not limited to unintentional data leakage and intentional data breaches. These types of data exposure represent just the tip of the iceberg. Another lesser-known data privacy harm—unauthorized data sharing by third-party technology vendors—can arise when businesses that rely heavily on an AI vendor's services to operate provide data to its generative AI tool. For instance, attorneys may be unwittingly exposing sensitive client data to government entities in their reliance on Westlaw's CoCounsel and LexisNexis's Protégé.[68] Both legal research vendors' parent companies, Thomson Reuters and RELX,

-neglect-ai-security-and-attackers-have-noticed/ar-AA1JBoLI?ocid [https://perma.cc/F5JB-TZ8T].

64. *Id.* The IBM report, Big Blue's Cost of a Data Breach Report 2025, contains findings from the self-reported responses of 600 global organizations. *Id.* The organizations reported security incidents that occurred between March 2024 and February 2025. *Id.*

65. *Id.*

66. *Id.*

67. *Id.* (noting that, of the organizations surveyed, "87 percent ha[d] no governance in place to mitigate AI risk [and] two thirds of those that were breached didn't perform regular audits to evaluate risk").

68. *See* Sarah Lamdan, *When Westlaw Fuels Ice Surveillance: Legal Ethics in the Era of Big Data Policing*, 43 N.Y.U. Rev. L. & Soc. Change 255, 257–58 (2019); *see also* Lizzie Bird, *LexisNexis's Contract with ICE as Unjust Enrichment*, 95 U. Colo. L. Rev. 1209, 1210 (2024) (discussing LexisNexis's contract with entities which allow LexisNexis to reveal data submitted to it).

currently have or recently had contracted with "local, state, and federal law enforcement entities, including ICE" to provide them with access to "billions of records of personal information aggregated from public and private sources."[69] In addition to legal research services, LexisNexis and Westlaw expanded their business models to include data broker services, which entail collecting and aggregating private and public data to build and maintain databases that serve as surveillance tools for "big data policing."[70] In fact, LexisNexis's 16.8 million dollar contract with ICE allowed agents to search LexisNexis's database in just seven months "over 1.2 million times, confirming fears that the data broker is 'enabling the mass surveillance and deportation of immigrants.'"[71]

---

69. *See* Bird, *supra* note 68, at 1210.

70. *See* Lamdan, *supra* note 68, at 257–58, 275 (explaining "[a]s commercial data brokers, [LexisNexis and Westlaw] aggregate and resell [] data . . . by purchas[ing] and consolidate[ing] the information held by individual data tracking firms, along with . . . data gleaned from public records, to create an information mosaic describing millions of people in great detail"). This aggregation and curation of personal data not only includes public records retained by local, state, and federal governments, but also data from online sources that track an individual's use of "social networks, blogs, chat rooms, lists of relatives and associates . . . ." *Id.* at 275.

71. Bird, *supra* note 68, at 1211. The backlash resulting from the LexisNexis contract with ICE is noteworthy. Students at law schools throughout the U.S. protested the contract and "called on LexisNexis to cut ties with ICE and on school administrations to cut ties with LexisNexis." *Id.* Additionally, more than forty immigrant advocacy and law school student organizations and "2,500 individuals—law professors, librarians, attorneys, and law students—" were signatories on a letter sent to the parent companies of LexisNexis and Westlaw. *Id.* The letter conveyed the signatories' demand that the companies halt their business relationship with ICE. *Id.* at 1212. The letter described the companies' relationship with ICE as one that enabled "the surveillance, imprisonment, and deportation of hundreds of thousands of immigrants each year" and allowed the companies to profit "from the misery being inflicted on immigrant communities by ICE." *Id.* at 1211–12. Significantly, despite public pressure from key consumer constituencies of the companies' legal research products, both RELX and Thomson Reuters continue to contract with law enforcement and immigration authorities. Lamdan, *supra* note 68, at 283. In stark contrast, IBM faced similar public and consumer pressure for its "interest in supplying surveillance products to ICE" but decided against "work[ing] on any projects that run counter to its values." *Id.*

Attorneys, especially those who represent clients in immigration matters, must consider whether utilizing Westlaw and LexisNexis's legal research and generative AI tools compromises their ethical obligations under Model Rule 1.6. A legal commentator critical of the relationship between Westlaw, LexisNexis, and law enforcement challenges attorneys to ask, "Is it possible that these [legal research companies] are sharing lawyers' research data with law enforcement?"[72] LexisNexis's generative AI tool, Protégé, claims "[c]ustomer data is only made available in the product context in which it has been entered and not shared with other [LexisNexis services] unless explicitly granted and communicated."[73] However, LexisNexis's primary legal research query tool, which is supported by extractive AI, does not have a similar express limitation on data sharing across LexisNexis products.[74]

Importantly, Westlaw's generative AI tool, CoCounsel, and its primary legal research query tool, powered by extractive AI, Westlaw Advantage, do not have privacy or AI governance policies that assure attorneys that client information provided in prompts, document uploads, or search queries is not shared across the company's varied services.[75] Thus, the "legal community should expect that the information they put into their Westlaw and LexisNexis accounts, including search histories and saved documents, is not confidential."[76]

Non-consensual data practices, vulnerability to data leakage, and the risk of unauthorized data sharing in generative AI tools are resounding reasons for attorneys to adopt such tools only with comprehensive and proactive data governance and privacy frameworks in place. The A.B.A. is best positioned to offer the legal profession a model approach for harnessing generative AI technology with those goals in mind. To understand whether the A.B.A.'s current guidance rises to this challenge, the following section re-examines an attorney's duty to protect the confidentiality of client information under the A.B.A.'s Model Rule of Professional Conduct 1.6. It also

72. Lamdan, *supra* note 68, at 260.
73. *Lexis+ AI Security Information*, *supra* note 49, at 9.
74. *See Privacy Policy*, *supra* note 46.
75. *See* Lamdan, *supra* note 68, at 290.
76. *Id.* at 290–91.

surveys the steps the A.B.A. has taken to date to guide attorneys on the use of generative AI technology in law practice, viewing those steps through the lens of confidentiality and data privacy.

III. The A.B.A.'s Approach to Artificial Intelligence

The A.B.A.'s response to AI advancement and integration into law practice has been largely reactive rather than proactive.[77] The profession it regulates has steadily adopted AI technology, while the A.B.A.'s official guidance has struggled to keep pace with technological changes to the practice of law, particularly compared to larger regulatory entities like the EU. The most consequential A.B.A. actions on AI technology began with resolutions that allowed it to act on the AI policies within them.[78] Those resolutions were followed by the creation of an AI Task Force, and finally culminated in its most recent formal opinion on AI. As the impact of AI and generative AI tools in the legal profession grows, bringing with it both promise and peril, attorneys must not only refamiliarize themselves with their obligation to keep client information confidential under Model Rule 1.6 ("Rule

---

77. Drew T. Simshaw, *Legal Ethics and Data Security: Our Individual and Collective Obligation to Protect Client Data*, 38 AM. J. TRIAL ADVOC. 549, 570 (2015). When Simshaw's article was published in 2015, the author noted the A.B.A. showed "tremendous leadership and pro-activeness in addressing … data security and ethics issues over the last few years," citing its formation of the Cybersecurity Legal Task Force in 2012, published educational materials, and other A.B.A.-sponsored technology resources. *Id.* Nevertheless, more than a decade has passed since then and in that time span the use of AI has steadily become prevalent in every aspect of society, including the legal profession. Yet, the Model Rules remain unchanged in the face of a profession changed by AI. Moreover, the A.B.A.'s consequential official actions are limited to several resolutions and one formal ethics opinion—all issued within the past six years—despite having formed its first committee on AI eighteen years ago. *See* A.B.A. TASK FORCE ON LAW AND A.I., ADDRESSING THE LEGAL CHALLENGES OF AI: YEAR 1 REPORT ON THE IMPACT OF AI ON THE PRACTICE OF LAW 1, 36 (Aug. 2024) [hereinafter AI Task Force Report], https://www.americanbar.org/content/dam/aba/administrative/center-for-innovation/ai-task-force/2024ai-taskforce-report-1-31-25.pdf [https://perma.cc/L4QS-7XRC (staff-uploaded, dark archive)].

78. *See* Jay D. Jerde, *ABA Resolutions: More Than Words*, ST. BAR WIS. (Mar. 26, 2025), https://www.wisbar.org/NewsPublications/InsideTrack/Pages/Article.aspx?Volume=17&ArticleID=30938 [https://perma.cc/R2K3-RCP4].

1.6)", but also understand how that duty has either adapted or failed to adapt enough to keep client information confidential.

A. The Duty of Confidentiality: Model Rule 1.6

In the age of generative AI, technology has largely outpaced the A.B.A.'s Model Rules of Professional Conduct.[79] The Model Rules were adopted in 1983, and since then, the rules have been occasionally amended, with the latest updates stemming from the A.B.A.'s Commission on Ethics 20/20.[80] The Commission's updates revitalized the rules "in response to technological developments and the globalization of legal practice."[81] The Model Rules' technological updates came well before the rapid evolution of AI and the birth of generative AI.[82] In its current form, Rule 1.6 focuses primarily on data security (transmission of client information via email and other communication devices) and stored data breaches (cloud computing), pre-generative AI.[83] It does not expressly consider an attorney's duty of confidentiality in conjunction with advanced AI systems.[84]

Rule 1.6 requires attorneys to keep client information confidential, stating, "a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent."[85]

---

79. Lamdan, *supra* note 68, at 285–86.

80. Katherine Medianik, *Artificially Intelligent Lawyers: Updating the Model Rules of Professional Conduct in Accordance with the New Technological Era*, 39 CARDOZO L. REV. 1497, 1511–12 (2018).

81. *Id.* at 1512.

82. *See id.* The Model Rules were updated more than a decade ago to "reflect the impact of technology on 21st Century law practice." *See* AI Task Force Report, *supra* note 77, at 15. The technology updates amended Model Rule 1.1 which addresses an attorney's competency to practice law. MODEL RULES OF PRO. CONDUCT r. 1.1 (A.B.A. 2025). Comment 8 of the rule specifically contemplates an attorney's technological skills and connects an attorney's competency to "keep[ing] abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engag[ing] in continuing study and education and comply[ing] with all continuing legal education requirements to which the lawyer is subject." *Id.*

83. *See* Simshaw, *Ethical Issues in Robo-Lawyering: The Need for Guidance on Developing and Using Artificial Intelligence in the Practice of Law*, 70 HASTINGS L.J. 173, 199–200 (2018).

84. *See* Medianik, *supra* note 78, at 1512.

85. MODEL RULES OF PRO. CONDUCT r. 1.6(a) (A.B.A. 2025).

The rule also provides that "a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[86] The A.B.A. amended the rule in 2012 to include the positive obligation of "reasonable efforts" and explained the language was added because "technological change has so enhanced the importance of this duty that it should be identified in the black letter and described in more detail [in the rule's comments]."[87] Comment 18 contemplates the rule's reasonable efforts requirement in detail by providing factors to consider when determining if an attorney has met their obligations under the rule:

> The sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty in implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[88]

Although an attorney's obligation to safeguard a client's information is subject to the "reasonable efforts" standard, the rule as adopted in many states also requires the attorney to do more than "reasonable efforts" if the client demands it.[89] Thus, to determine if a client demands more stringent safeguards, "it is important for lawyers to have candid conversations with their clients in which they discuss the practice's use of technology and the associated risks."[90] In fact, candid client conversations are not just important to have, attorneys are required to have these conversations under Model Rule 1.4 ("Rule 1.4")—the duty of communications.[91] Rule 1.4 obligates an attorney to consult with their client about how the attorney will represent the client and obtain their client's informed consent for decisions related to carrying out the goals or objectives of representation.[92]

---

86. MODEL RULES OF PRO. CONDUCT r. 1.6(c) (A.B.A. 2025).

87. Simshaw, *supra* note 77, at 559.

88. *Id.*; *see* MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18 (A.B.A. 2025).

89. *See* Simshaw, *supra* note 77, at 560.

90. *Id.*

91. *Id.*; *see* MODEL RULES OF PRO. CONDUCT r. 1.4 (A.B.A. 2025).

92. MODEL RULES OF PRO. CONDUCT r. 1.4 (A.B.A. 2025).

In addition to considering their client's preference regarding information security, because Rule 1.6 only denotes a baseline standard of ethical conduct for attorneys regarding confidentiality, attorneys should also follow data security best practices which, often go beyond the rule's minimum requirements.[93] Furthermore, because the definition of what "reasonable efforts" are under the rule will change as technology advances, an ethics opinion issued by Arizona's state bar on "satisfying the duty to take reasonable security precautions" cautioned its attorneys to conduct "periodic reviews to ensure that security precautions in place remain reasonable as technology progresses."[94] Other states' ethics opinions on cloud computing are also illustrative of an attorney's obligation to protect the confidentiality of client information and "how ethics boards treat the use of new technology by lawyers."[95] An Ohio ethics opinion, for example, determined "lawyers may use cloud services as long as they competently select an appropriate vendor, preserve confidentiality, [and] safeguard client property . . . ."[96] Iowa, New Jersey, and North Carolina opinions demand more stringent security measures of attorneys such as an evaluation of a cloud computing vendor's level of protection for client information or its use of current technology to protect against data breaches.[97]

Even with Rule 1.6, its comments, and formal ethics opinions interpreting the Rule, attorneys in the age of AI are left without clear and consistent guidance on its use, given that the Rule's last update was more than a decade ago. The Rule and its purported built-in flexibility to adapt to evolving technologies do not hold up against the pronounced privacy harms that the use of generative AI in law practice can pose to a client's personal data and confidential information. As one data security legal scholar aptly surmised in urging state bar associations to adopt the A.B.A.'s most recent technology-related amendments, "clients are counting on bar associations and ethics bodies to continue to fulfill this critical role of helping lawyers prevent

93. *See* Simshaw, *supra* note 77, at 565.
94. *Id.* at 561–62.
95. *Id.* at 564.
96. *Id.*
97. *Id.* at 565.

breaches of their confidential information."[98] This assertion remains true in the age of AI; attorneys and clients are counting on the A.B.A. to help guide them through AI's transformation of the legal profession. To that end, in 2019, the A.B.A. began ramping up its efforts to provide relevant guidance to attorneys on the ethical use of AI and generative AI in the practice of law with the passage of several resolutions on the topic.

B. Resolutions 112 and 604

The A.B.A.'s initial responses to advancements in AI technology and its integration into law practice were a series of formal resolutions adopted by its House of Delegates.[99] Resolutions 112, 700, and 604 address how attorneys, the courts, regulators, and other stakeholders utilize AI technology.[100] Resolution 700 deals with pre-trial risk assessment tools and tasks entities within the justice system to "refrain from using [the tools] unless the data supporting the risk assessment is transparent, publicly disclosed and validated to demonstrate the absence of conscious or unconscious racial, ethnic or other demographic, geographic or socioeconomic bias."[101] Although Resolution 700 concerns data and AI technology, it is solely focused on ensuring the data used in pre-trial assessment tools is free of bias.[102] For purposes of this Article, Resolutions 112 and 604 more directly consider the privacy risks analyzed here and their relationship with the Model Rules of Professional Conduct.

1. Resolution 112

Resolution 112, passed in August 2019, calls on attorneys and courts "to address ethical and legal issues arising from the use of AI in the practice of law."[103] Specifically, it emphasizes attorneys should consider the "ethical and beneficial usage of AI . . . and . . . controls and oversight

---

98. *Id.* at 572.

99. *ABA House Adopts 3 Guidelines to Improve Use of Artificial Intelligence*, A.B.A. (May 23, 2023), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/may-23-wl/ai-0523wl/ [https://perma.cc/9AWD-HP6J (staff-uploaded, dark archive)].

100. *Id.*

101. *Id.*

102. *See* Adopted Resol. 700 (A.B.A. 2022).

103. Adopted Resol. 112 (A.B.A. 2019).

of AI and the vendors that provide AI."[104] The report accompanying the resolution further articulates the A.B.A.'s intent to explore whether it should promulgate "a model standard" for adoption by the House of Delegates.[105] Notably, the report describes the ways AI is used in the practice of law, but does not list the use of generative AI because the technology was not available to attorneys at the time of the resolution's adoption.[106] The report specifically identifies four Model Rules of Professional Conduct that apply to the use of AI.[107] The duty of confidentiality and communications appears among the listed ethical rules. Regarding confidentiality, the report highlights an attorney's obligation to take "reasonable efforts" to safeguard a client's information.[108] It acknowledges the use of AI tools may require "sharing" of client information with third-party vendors and reminds attorneys to investigate AI vendors' data security and storage measures, and data access protocols.[109] Additionally, it warns attorneys not to use AI tools in the representation of a client "unless the [attorney] is confident the client's confidential information will be secure."[110]

On the duty of communications front, the report stresses that an attorney's duty under the rule requires a discussion with a client about how the attorney plans to use AI while representing the client before the decision to use AI is made.[111] This discussion must account for the risks, benefits, and limitations associated with AI use.[112] Only after this type of discussion can an attorney obtain a client's informed consent for the attorney to use AI.[113]

---

104. *Id.*

105. *Id.* at 1.

106. *See id.* at 2–4. The resolution's report identifies seven categories of AI use in the practice of law. *Id.* Those categories include electronic discovery and predictive coding, litigation analysis and predictive analysis, contract management, due diligence reviews, "wrongdoing" detection, legal research, and detection of deception. *Id.*

107. *Id.* at 4–7.

108. *Id.* at 6.

109. *Id.*

110. *Id.*

111. *Id.* at 5–6.

112. *Id.*

113. *Id.*

Additionally, a brief discussion about privacy appears in the resolution's report.[114] The primary concerns highlighted relate to the use of AI for automated decision-making about people (e.g., home loan approval, receipt of health benefits, or employment decisions) and to monitor people in the workplace.[115] There is also a cursory mention of data privacy laws, like the EU's General Data Protection Regulation ("GDPR"). The report indicates an attorney's AI use might trigger compliance requirements under certain privacy laws, and thus, attorneys or law firms should conduct an "AI analysis" to ensure they comply with those laws' requirements.[116]

A noteworthy section follows the individualized sections on the four applicable ethical rules. It gives "key practical takeaways relating to the ethics of AI."[117] Here, the authors suggest the profession's model rules are equipped to provide attorneys sufficient guidance regarding the use of AI technology since "the ethical issues raised by AI are simply a permutation of ethical issues lawyers have faced before with regard to other technology."[118] This assertion seems to contradict the report's earlier statement indicating the A.B.A. would consider whether a new "model standard" should be promulgated in light of AI's integration into the practice of law.[119] Moreover, the subsequent adoption of Resolution 604 implies the Model Rules and their guidance were not up to the task of providing sufficient guidance on the use of AI technology.

2. Resolution 604

Resolution 604, passed in February 2023, expands on Resolution 112's call to action because it includes not only attorneys and law firms, but also "organizations that design, develop, deploy, and use AI" in its scope.[120] The subject matter focus of Resolution 604 revolves around "human authority, oversight, and control," "transparency and traceability," and "responsibility for consequences, injury, or harm" of

114. *Id.* at 11.
115. *Id.* at 10–11.
116. *Id.*
117. *Id.* at 7.
118. *Id.*
119. *Id.* at 1.
120. Adopted Resol. 604, 4 (A.B.A. 2023).

AI systems.[121] Additionally, it calls on other governing bodies like the U.S. Congress, executive agencies, and state legislatures to formulate regulations similar to those contained in the A.B.A.'s resolution.[122] The report accompanying the resolution explains the reasoning behind the resolution's subject matter focus: "This Resolution will help to ensure that accountability, transparency, and traceability are built into AI . . . systems . . . 'by design' from the beginning of the development process . . . [thus] maximizing the benefits from the use of AI in a trustworthy and responsible manner and . . . minimiz[ing] the risks.[123] Furthermore, the report recognizes the importance of protecting the American public as AI technology infiltrates every aspect of society, citing to The White House Office of Science and Technology Policy's ("OSTP") purpose for creating a Blueprint for an AI Bill of Rights, which states the blueprint was drafted, "for building and deploying automated systems that are aligned with democratic values and protect civil rights, civil liberties, and privacy."[124]

Regrettably, besides this particular reference to privacy, the term "privacy," or any discussion of AI technology and the risk it poses to sensitive personal or business information, is few and far between.[125] In fact, the term "privacy" appears just sixteen times in the 23-page document.[126] The phrase "sensitive personal information" appears only once.[127] And, when the term or phrase appears in the report, it is paired

---

121. *Id.* at 1, 4.

122. *Id.* at 2.

123. *Id.*

124. *Id.* at 3–4 (further quoting The White House Office of Science and Technology Policy, "Our country should clarify the rights and freedoms we expect data-driven technologies to respect. What exactly those are will require discussion, but here are some possibilities: . . . your freedom from pervasive or discriminatory surveillance and monitoring in your home, community, and workplace; and your right to meaningful recourse if the use of an algorithm harms you").

125. *See generally* Adopted Resol. 604, *supra* note 120 (the document recognizes AI use triggers privacy considerations but a privacy analysis is not the focus of the resolution's report).

126. *See generally id.* Data privacy is mentioned in a report footnote identifying other areas of concern associated with the use of AI which may be the subject of future ABA resolutions. *Id.* at 2 n 6.

127. *Id.* at 7 (commenting on the passage of the California Consumer Privacy and California Privacy Rights Acts).

with minimal analysis or commentary. The sparse treatment of privacy in Resolution 604 and its report highlights a gap in the A.B.A.'s early approach to AI governance. Although Resolution 604 outlined broad principles for accountability and responsible AI use, the A.B.A. again expanded its efforts by creating the Presidential Task Force on Law and Artificial Intelligence.

C. Artificial Intelligence Task Force

In August 2023, the A.B.A. created the A.B.A. Presidential Task Force on Law and Artificial Intelligence.[128] The AI Task Force identified three areas to focus its efforts: "(1) address the impact of AI on the legal profession and the practice of law, and related ethical implications (2) provide insights on developing and using AI in a trustworthy and responsible manner, and (3) identify ways to address AI risks."[129] At the outset, one of the Task Force's primary goals was to evaluate ethical concerns related to AI since "practitioners and judges remain focused on the need to protect client confidentiality."[130] As part of its work, the Task Force provided an AI education webinar series, published a book on AI that offers legal analysis and practical advice, and conducted an education survey designed to evaluate law schools' integration of AI into legal education.[131]

Following a year of work, the Task Force issued its first report about the impact of AI on the profession.[132] The report prefaces its consideration of several ethical rules' application to AI use with an assertion that "although the A.B.A. Model Rules were not written to address specific technologies, they are comprehensive enough to permit the responsible and ethical use of [generative AI] tools in legal practice."[133] Regarding the duty of confidentiality, the report warns attorneys to use caution when using confidential client information in

128. AI Task Force Report, *supra* note 77, at 1.

129. *Id.* at 3.

130. *Id.* at 4.

131. *Id.*

132. AI Task Force Report, *supra* note 77.

133. *Id.* at 15. The ethical rules covered in the Task Force's report include fees/billing, competence, deepfakes and candor toward the court, responsibility for lawyers' agents, confidentiality, diligence, consultation, communication, and competence. *Id.* at 15–17.

a prompt to a generative AI tool.[134] It explains that, because many generative AI tools do not provide confidentiality for the information provided in prompts (i.e., the AI models train on information gained from user prompts which can reveal that information to others) attorneys "must understand how information submitted in a prompt will be used and shared and also where it will be stored . . . [because] [t]he [lack of] data security of AI model companies and law offices using these products can put [client information] . . . at risk."[135]

Significantly, the report's consideration of confidentiality amounts to three brief paragraphs. It does, however, provide slightly more discussion about the risks to personal data posed by generative AI in a section dedicated to privacy and cybersecurity.[136] Its privacy discussion underscores the immense amount of personal data AI systems rely on to operate.[137] Additionally, it entails a more detailed description of the ways in which AI systems can consume and then exploit personal data.[138] As it relates to generative AI and its ability to enhance AI systems' already powerful capabilities, the report identifies the potential for significant privacy harms resulting from the surveillance and identification of individuals by using enhanced AI systems "'abilities . . . to sort through hundreds of thousands of emails, texts, documents, and more to identify individuals such as whistleblowers [and] potential targets of law enforcement investigations . . . .'"[139] In that same vein, the report describes generative AI systems' mass data scraping practices that sweep in the data of individuals who are unaware their data is being collected and repurposed for unpermitted uses.[140] In recognizing these specific privacy harms associated with generative AI use, the report suggests a

134. *Id.* at 16 (qualifying this warning with the phrase "without a client's informed consent").

135. *Id.*

136. *See id.* at 28.

137. *See id.*

138. *Id.*

139. *Id.*

140. *Id.* (describing an additional privacy harm related to non-consensual data collection, where companies or governments could "create digital dossiers that could be used to generate content geared to an individual's inclinations (from customized marketing to influencing the way the person votes)").

legal vacuum or ethically gray area exists for generative AI vendors to do business in.[141] And, the report notes that even if laws exist, they "lack teeth" or are "silent on how personal data should be collected and used in a way that preserves privacy."[142]

The Task Force's second report, issued in December 2025, marks the conclusion of the Task Force's work and reiterated the data privacy and ethical concerns raised by AI and generative AI use in legal practice.[143] Specifically, legal and judicial experts predicted the A.B.A. may "craft ethical frameworks to ensure that AI enhances and does not undermine the integrity of the legal and justice systems" and "concerns over confidentiality and data privacy will result in efforts to establish regulations and enact policies and protocols aimed at safeguarding confidential information from unintended exposure or misuse."[144]

In light of these privacy risks and the absence of robust legal safeguards in the United States, the A.B.A., through Formal Opinion 512, further examined the ethical obligations of attorneys related to the use of generative AI tools.

D. Formal Ethics Opinion 512

The A.B.A.'s Standing Committee on Ethics and Professional Responsibility issued its first formal opinion on the use of generative

---

141. *Id.*

142. *Id.*

143. A.B.A Task Force on L. & A.I., *Addressing the Legal Challenges of AI: Year 2 Report on the Impact of AI on the Practice of Law*, 1 (Dec. 2025), https://www.americanbar.org/content/dam/aba/administrative/center-for-innovation/ai-task-force/2025-ai-task-force-year2-report.pdf [https://perma.cc/626Z-9WLH (staff-uploaded, dark archive)]. With the Task Force's disbandment, its work will be reallocated to the ABA's Center for Innovation. *Id.* at 5. The ABA Center for Innovation plans to continue the Task Force's charge to navigate rapidly evolving AI technologies by using a strategic plan "centered around three core functions: Connecting, Convening, and Curating. The[] '3 Cs.'" *Id.* at 5. The first two Cs aim to connect and convene ABA members and experts to address AI issues affecting legal practice. *Id.* The third C seeks to provide ABA members with "AI resources" by "aggregating AI content developed by the AI Task Force and other ABA entities." *Id.*

144. *Id.* at 20 (quoting Judge Scott Schlegel, Maura Grossman & Judge Herbert B. Dixon on the responsible use of AI and ethical frameworks).

AI tools in July 2024.[145] Formal Opinion 512 focuses solely on an attorney's use of generative AI tools and identifies eleven applicable ethical rules for discussion in the opinion.[146] For purposes of this Article, the opinion's analysis of Rule 1.6 (confidentiality) and Rule 1.4 (communications) is explained here.

On Rule 1.6, the opinion begins by reminding attorneys that the rule requires an assessment of the "nature and extent of the risk" to confidential client information when using generative AI tools.[147] The assessment must include an evaluation of "the likelihood of disclosure and unauthorized access, the sensitivity of the information, the difficulty of implementing safeguards, and the extent to which safeguards negatively impact the lawyer's ability to represent the client."[148] To that end, the opinion recognizes that "[s]elf-learning [generative AI] tools into which lawyers input information relating to representation, by their very nature, raise the risk that information relating to one client's representation may be disclosed improperly . . . [to others inside or outside the firm using the same tool]."[149] Therefore, the opinion determines an attorney's use of generative AI tools

145. A.B.A. Comm. on Ethics & Pro. Resp., Formal Op. 512 Generative Artificial Intelligence Tools (2024) [hereinafter A.B.A. Comm. on Ethics & Pro. Resp.].

146. *Id.* at 1–2. In the fifteen-page opinion, eleven ethical rules are discussed: competence (1.1); confidentiality (1.6, 1.18(b), and 1.9(c)); communications (1.4); fees (1.5); supervision of non-lawyer assistance (5.1 and 5.3); meritorious claims and contentions (3.1 and 3.3); and candor toward the tribunal (8.4(c)). *Id.* at 2–14.

147. *Id.* at 6.

148. *Id.*

149. *Id.* at 6–7 (citing to the State Bar of Cal. Standing Comm. on Prof'l Resp. & Conduct, PRACTICAL GUIDANCE FOR THE USE OF GENERATIVE ARTIFICIAL INTELLIGENCE IN THE PRACTICE OF LAW (2024); Fla. Bar Ethics. Op. 24–1 (2024). Just eighteen states and the District of Columbia have issued legal ethics opinions, resolutions, guidance, or reports and recommendations related to AI. *See Legal Profession Comparison Table – State Legal Ethics Guidance on Artificial Intelligence (AI)*, BLOOMBERG L., htttps://www.bloomberg.com/external/document/X2JK49QC000000/legal-profession-comparison-table-state-legal-ethics-guidance-on [https://perma.cc/D9R5-C5EU] (last visited Aug. 18, 2025). Those states include: Alaska, California, Florida, Kentucky, Michigan, Minnesota, Mississippi, Missouri, New Jersey, New Mexico, New York, North Carolina, Oregon, Pennsylvania, Texas, Virginia, and West Virginia. *Id.*

requires the informed consent of the client "prior to inputting information relating to the representation into [a self-learning] [generative AI] tool."[150]

Additionally, the opinion further qualifies the use of generative AI tools even with the informed consent of the client:

> Because of the uncertainty surrounding [generative AI] tools' ability to protect such information and the uncertainty about what happens to information both at input and output, it will be difficult to evaluate the risk that information . . . will either be disclosed to or accessed by others . . . . As a baseline, all lawyers should read and understand the Terms of Use, privacy policy, and related contractual terms and policies of any [generative AI] tool they use to learn who has access to the information . . . input[ed] into the tool or consult with a[n]. . . expert [about] those terms and policies . . . [and how] [generative AI] tools utilize information.[151]

The opinion's duty of communication analysis re-emphasizes an attorney's responsibility to obtain the informed consent of the client to utilize a generative AI tool during representation.[152] Moreover, it provides that an attorney's communication with the client will largely depend on the facts or circumstances related to representation and the "sensitivity of the information" to be used in the generative AI tool.[153] The opinion completes its consideration of client communication by noting that there may be instances where the duties of Rules 1.4 and 1.6 will not apply to an attorney's use of generative AI tools.[154] However, it recommends disclosing the use of generative AI tools to

150. A.B.A. Comm. on Ethics & Pro. Resp., *supra* note 145, at 7.

151. *Id.*

152. *Id.* at 8 (explaining "Model Rule 1.4(b) obligates lawyers to explain matters 'to the extent reasonably necessary to permit a client to make an informed decision regarding the representation'").

153. *Id.* at 8–9.

154. *Id.* at 9.

clients at the outset, regardless of the rules' application, to foster greater trust and open communication.[155]

The opinion's discussion of confidentiality and communications provides little in the way of new guidance on AI. Instead, it offers some education on the pitfalls of entering client information into generative AI tools and a reiteration of the rules' timeworn language tied to the use of generative AI. While A.B.A. Formal Opinion 512 relies on existing ethical rules to govern the use of AI, the EU has taken a more forward-looking stance by enacting the world's foremost comprehensive regulatory framework for AI and data protection.

IV. The EU's Approach to Artificial Intelligence

In stark contrast to the U.S. and its governmental and professional regulatory bodies, the EU is one of the first early adopters of AI regulation.[156] The driving force behind its leadership in this area is derived from the European Union Charter of Fundamental Rights ("The Charter").[157] Respect for an individual's private life and protection of personal data are among the rights enshrined in The Charter.[158] These rights and others laid the foundation for the EU's data privacy and AI regulations.[159]

A. The Artificial Intelligence Act

The EU's AI Act ("AIA"), passed in 2023, creates a regulatory framework for AI systems that imposes scaled requirements based on a technology's level of risk.[160] This risk-based AI classification system

155. *Id.* (also noting that boilerplate language in a retainer agreement will not suffice as an explanation worthy of obtaining the client's informed consent to use generative AI during representation).

156. Maroussia Lévesque, *Smoke and Mirrors? Corporate Discretion in AI Regulation*, 2025 U. Ill. J. L. Tech. & Pol'y 33, 48.

157. Hillman, *supra* note 21, at 783.

158. *Id.*

159. *Id.* Other fundamental rights contained in The Charter that provide a foundation for data privacy and AI regulations in the EU include the right to human dignity, freedom from discrimination, gender equality, freedom of expression and assembly, the right to a defense and a presumption of innocence, fair and just working conditions, the rights of a child, the inclusion of people with disabilities, and environmental protection. *Id.*

160. Lévesque, *supra* note 156, at 46–48.

has four tiers: unacceptable risk, high risk, limited risk, and minimal risk.[161] It applies to both providers (entities that place an AI system or service on the market) and deployers (users of AI systems except for solely personal, non-business users) of AI systems.[162] The purpose of the AIA is "to establish trustworthy AI and to develop 'high quality,' transparent AI models."[163] Moreover, the AIA is a response to the growing and apparent need for a structured, unified, and comprehensive AI governance framework that would "avoid inconsistent AI laws in the EU, which would hinder the development of AI by 'fragment[ing]' the market."[164] Although the AI classification system firmly holds certain types of AI systems in a specific tier, the AIA is also designed to provide flexibility as AI technology develops.[165] Each EU member state has a regulatory entity with oversight, reporting obligations, and enforcement powers, and an "overarching European Union Artificial Intelligence Board comprise the structured enforcement body" of the AIA.[166]

The member states' regulatory entities and the EU AI Board assign certain regulations for each AI risk level category—the higher the risk level, the more stringent the regulations.[167] For instance, the unacceptable risk category, which includes AI designed to provide social scoring for governments, claims the most stringent regulation: a

161. *Id.* at 49.

162. Sandra Wachter, *Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond*, 26 YALE J.L. & TECH. 671, 677 (2024).

163. Hillman, *supra* note 21, at 783.

164. *Id.* at 783.

165. *Id.* Under the AIA, its enforcement bodies may revisit the classification categories (add or remove AI systems) as the technology progresses. *See* Wachter, *supra* note 162, at 713, 716.

166. Eur. Parl., *EU AI Act: First Regulation on Artificial Intelligence* [hereinafter EU AI Act], https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence [https://perma.cc/7D3R-FXWS] (last updated Feb. 19, 2025); *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations*, COM (2024).

167. EU AI Act, *supra* note 166.

complete ban.[168] AI systems in the high-risk category include those AI systems that are "intended to be used as a safety component of a product, or [where] the AI system is itself a product" (medical devices and toys) and (2) eight other high-risk applications: biometrics including emotion recognition; critical infrastructure; education and vocational training; employment, employee management, and access to self-employment; access to and enjoyment of essential private services and essential public services and benefits; law enforcement; migration, asylum, and border control management; and administration of justice and democratic processes.[169]

---

168. *Id.* The AIA's Article 5 also prohibits the following AI systems in the unacceptable risk category

> - subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques;
> - an AI system that exploits any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability, or a specific social or economic situation;
> - biometric categorization systems that categorize individual[] natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation (exceptions apply for law enforcement);
> - real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement, unless strictly necessary for certain objectives;
> - risk assessments of natural persons to assess or predict the risk of a natural person committing a crime, based solely on the profiling of a natural person or on assessing their personality traits and characteristics;
> - AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage;
> - AI systems to infer emotions of a natural person in the workplace and education institutions, except where the use of the AI system is intended for medical or safety reasons.
>
> Commission Regulation 2024/1689, art.5, 2024 O.J. (L 1689).

169. Commission Regulation 2024/1689, art.6(1(a)), 2024 O.J. (L 1689).

AI system use in these areas are not prohibited but are subject to compliance requirements.[170] Compliance requirements for providers of these systems include but are not limited to "duties such as establishing risk-assessment systems; ensuring data governance; keeping technical documentation and records; and maintaining transparency, human oversight, accuracy, cybersecurity, and robustness."[171] High-risk AI systems must also conduct a fundamental human rights impact assessment.[172] Deployers' compliance requirements are less strict and consist only of "human oversight, recordkeeping, and monitoring duties, and for some deployers, [a] fundamental rights impact assessment."[173] AI systems in the limited or minimal risk categories are not regulated like high-risk AI systems.[174] Instead, AI systems that fall into the limited risk category must follow transparency and disclosure requirements, which entail notifying individuals when they are interacting with AI technology such as AI-powered chatbots or content that is AI-generated.[175] And finally, those AI systems in the minimal risk category are allowed to voluntarily participate in the AIA's requirements or codes of conduct.[176]

The AIA specifically addresses provider and deployer obligations relating to generative AI systems.[177] All providers of generative AI systems must "draw up and keep up-to-date the technical documentation of the model, including its training and testing process and the results of its evaluation . . . ."[178] Providers must also disclose certain information to downstream providers, respect copyright law,

170. *Id.* annex III.

171. *Id.* arts. 9–15.

172. *Id.* art. 27(2). The AIA's human rights assessment requirement only applies to providers or deployers in the public sector. *Id.* art. 27(1).

173. *Id.*

174. *Id.* art. 4.

175. *Id.*

176. *Id.* art. 5.

177. *Id.* at art. 2(1); *id.* arts. 50, 71. The original draft of the AIA was silent on provider and deployer use of generative AI systems. *See* Wachter, *supra* note 160, at 694. Although the AIA passed with provisions regulating generative AI, the lobbying efforts of several nations, including France (the country of origin for the generative AI tool Mistral), produced a watered-down version of those GAI provisions. *Id.* at 694–95.

178. EU AI Act, *supra* note 166, art. 53.

[and] provide a sufficiently detailed summary of the training data . . . ."[179] The AIA distinguishes between generative AI systems with and without systemic risks.[180] Systemic risks include but are not limited to "any actual or reasonably foreseeable negative effects on democratic processes, public and economic security."[181] Those AI systems with systemic risks are more regulated than those without.[182] Unfortunately, commonly used generative AI tools like the subscription-free ChatGPT, Anthropic's Claude, and others do not qualify as such despite their potential for systemic risk.[183] However, ChatGPT's subscription service qualifies as an AI model with the potential for systemic risk which requires its provider, OpenAI, "to perform model evaluations—including adversarial testing (e.g., red teaming) that does not need to be external—assess and mitigate possible systemic risks, document and report serious incidents and possible corrective measures, and ensure an adequate level of cybersecurity."[184]

The AIA's risk-based classification framework and its enforcement mechanisms are just the newest tools in the EU's AI regulation toolkit. Long before the AIA's inception, the EU developed and enacted the GDPR, the world's foremost data privacy and protection framework.

B. General Data Protection Regulation

The AIA does not operate alone. Rather, it complements an already robust data privacy and technology regulatory framework in the EU. Prior to the AIA's passage, the EU's GDPR was adopted in 2016 and became effective in 2018.[185] Under the GDPR, which offers EU citizens a rights-based approach to privacy, "the consumer owns their

179. *Id.*

180. Wachter, *supra* note 162, at 696–98.

181. *Id.*

182. *Id.*

183. *Id.* (critiquing the AIA's governance of generative AI as "[D]isappointing. The two-tier model is quite unconvincing because many 'systemic risks' occur in all GPAI models, regardless of their size or computation. Misinformation, hallucinations, bias, work displacements, data protection issues, explainability problems, and harmful outcomes occur in smaller and less 'capable' systems").

184. *Id.* at 696–97.

185. Chang, *supra* note 30, at 29.

personal information and 'presumptively [has] the legal right to control [the information]' and who or what uses it."[186] Therefore, any company can only collect and process an EU individual's data under the GDPR if one of the following applies

> (1) the data subject consents; (2) processing is necessary to perform a contract to which the data subject is party; (3) processing is necessary to perform a legal obligation; (4) processing is necessary to protect the vital interests of the data subject or of another person; (5) processing is necessary to perform a task that is in the public's interest; or (6) processing is necessary for legitimate interests pursued by the company or a third party.[187]

In addition to the restrictions placed on personal data collection and processing, the GDPR provides individuals with a set of data access and control rights that include: the right to access and inspect data, the right to request correction of data inaccuracies, the right to portability or transfer of data from one entity to another, the right to consent to the sale of personal data or for data to be used to receive targeted advertisements, and the right to appeal a company's denial of an individual's data request.[188] Other key governing principles of the GDPR focus on data minimization, transparency, data impact protection assessments, employee data privacy training, and sufficient record keeping of data collection and use.[189]

On the AI front, the GDPR "gives the EU tools to combat civil rights and economic justice issues that can result from the inappropriate use of personal data in AI systems."[190] Before generative AI, the GDPR aimed to prevent discriminatory AI automated decision-making in receipt of public and private services (home loan

186. Cook & Mavrova Heinrich, *supra* note 10, at 356.
187. *Id.*
188. *Id.*
189. *Id.* at 357.
190. Hillman, *supra* note 21, at 808–09.

approval, employment decisions, etc.).[191] "The GDPR requires processors of personal data to provide 'meaningful information about the logic involved' in algorithmic decision-making, which includes a description of '(1) the categories of data used in processing; (2) the relevance of the data; (3) how profiles are built; (4) the relevance of the profile to the decision-making process; (5) and how the profile is used for an individualized decision.' "[192]

Following the introduction of generative AI, international efforts to regulate generative AI using the GDPR have focused on an AI system's data processing and collection instead of automated decision-making.[193] An enforcement action by Italy's Data Protection Authority ("IDPA") against ChatGPT identified specific concerns regarding transparency in data processing, the legal basis for data collection, the accuracy of generated information, and safeguards for minors.[194] Consequently, the IDPA halted ChatGPT's operation in Italy and "set forth a series of corrective measures for OpenAI . . . requir[ing it] to enhance transparency by clarifying data processing methods and users' rights, ensure data processing had a legitimate legal basis, and provide mechanisms for data subjects to exercise their rights, such as correcting or deleting inaccurate data."[195] Following OpenAI's compliance with the IDPA's demands, ChatGPT resumed operations in Italy.[196] This enforcement of the GDPR showcases that a regulatory body's "proactive stance" paired with an AI provider's cooperation with compliance can "set a precedent for international AI governance [and] exemplifies the potential for . . . AI developers, users, and regulatory bodies work[ing] together to achieve a balance between protecting personal rights and fostering technological advancement."[197]

---

191. *See generally* Cook & Mavrova Heinrich, *supra* note 11, at 356–58 (describing GDPR data collection and processing provisions applicable to U.S. companies).

192. Hillman, *supra* note 21, at 809.

193. Chang, *supra* note 30, at 42.

194. *Id.*

195. *Id.*

196. *Id.* at 43.

197. *Id.*

V. AN EU MODEL FOR THE A.B.A.'S MODEL RULES OF PROFESSIONAL CONDUCT

"Professional regulation of lawyers has a variety of purposes, including the provision of guidance to lawyers [and courts], and the maintenance of a public image that fosters client trust . . . ."[198] Although the Model Rules still provide a modicum of useful guidance for attorneys, as do the A.B.A.'s resolutions and formal ethics opinion on AI, they fall short of adequately instructing attorneys on how to properly safeguard client information in the age of AI. Now is the time for the A.B.A. to update its Model Rules, and to expressly and adequately account for the rapid advancement of AI technology and global governance frameworks designed to regulate it. As one legal scholar advocated, "if properly utilized by the legal profession as a whole, attention to and promotion and enforcement of legal ethics rules could have a profoundly positive effect on proactively improving data security in the practice of law."[199] The A.B.A. acknowledges that it is "uniquely positioned to assess [AI opportunities and challenges] and to help ensure [AI's] integration [into law practice] is ethical and responsible and serves the public good."[200]

Therefore, the limitations of Rule 1.6 in addressing the risks to personal data posed by attorneys' use of generative AI tools should be rectified by amending the rule to reflect the EU's AI Act and GDPR. EU laws have affected the use of AI tools and data privacy practices in the United States.[201] Known as the "Brussels Effect," the EU's leadership in this area often serves as a blueprint for regulations in other jurisdictions.[202] More than 448 million people in twenty-seven countries reside in the EU, "making [it] one of the world's biggest markets."[203] If attorneys and legal organizations want to remain

198. Medianik, *supra* note 80, at 1512.

199. Simshaw, *supra* note 77, at 554–55.

200. AI Task Force Report, *supra* note 77, at 3.

201. Wachter, *supra* note 162, at 676. In the United States, California became an early adopter of the EU's GDPR when it modeled its California Consumer Privacy and California Privacy Acts after the GDPR's provision of individual data rights and data controller compliance requirements. *See* Cook & Mavrova Heinrich, *supra* note 11, at 353–54.

202. *Id.*

203. Wachter, *supra* note 162, at 676.

competitive in a global market, then they will have to comply with these laws.[204]

Instead of allowing a piece-meal, fragmented approach—where individual law practices, legal organizations, and state bar associations develop their own AI and data privacy rules—the A.B.A. must step in to regulate conduct, as the EU's regulatory body has done, to achieve a structured, unified, and comprehensive framework for AI use and data privacy that preserves client privacy and confidential information. Even the A.B.A.'s guidance on AI and generative AI is scattered among various official documents and publications. This inconsistent and disjointed approach, which fails to align with global best practices for AI governance, will likely slow the integration of generative AI tools into legal practice and significantly limit the profession's ability to harness the substantial benefits of the technology.

A modernized Model Rule 1.6 (and other model rules) will offer the legal profession a one-stop shop for AI guidance. Consequently, modernization will likely foster attorneys' confidence and trust in harnessing the advantages of AI technology because attorneys will not have to enter a minefield of ethical and legal risk. Additionally, clients will be more apt to support and trust an attorney's use of AI during a representation with a modernized A.B.A. guardrail in place.

A. Proposal: Create a Categorized AI Risk-Based Assessment Framework Modeled After the EU's Artificial Intelligence Act and General Data Protection Regulation

To modernize Rule 1.6, the A.B.A. should include specific language that requires attorneys to conduct a categorized AI risk-based assessment prior to and during their use of AI and generative AI to avoid compromising confidential client information through "the inadvertent or unauthorized disclosure of, or unauthorized access to,

204. *Id.* (commenting on the passage of the AIA, the world's first comprehensive and legally enforceable AI law, "from a business perspective, and in the interest of streamlining, it will make sense for businesses to adapt their operations to comply with the strictest laws rather than to have fragmented standards across operations.").

information relating to the representation of a client."[205] In addition to amending the rule's language, the comments to the rule should contain detailed guidance on the substance and application of a categorized AI risk-based assessment. The categorized AI risk-based assessment would not be AIA-compliant in a strict or legal sense, nor would it follow the Act's language verbatim; rather, it would provide a framework that categorizes lawyering tasks involving AI and generative AI tools—used for specific purposes and with specific types of data—into tiered risk levels that mirror the structure of the AIA's system.

Take, for example, an attorney (AI deployer) who plans to draft a memo (lawyering task) for their supervising partner and client in a medical malpractice matter (specific purpose) utilizing Westlaw's CoCounsel (AI provider). A categorized AI risk-based assessment here might fall into the limited risk category if the attorney does not provide CoCounsel with the client's sensitive medical data, personal identifying information, or utilize data de-identifying or anonymization practices before sharing information with the AI tool. Therefore, transparency and disclosure obligations, such as communicating AI use to the client, the purpose for it, and any information that might be shared with the AI tool, would apply in this instance.

However, should the attorney include personal data or sensitive information in a prompt or document uploaded to CoCounsel, even with the client's informed consent, then the use of generative AI could be reclassified as high-risk. In that case, the attorney would follow privacy and data protection requirements that closely mimic the AIA's compliance requirements for high-risk AI systems. Those requirements include ensuring data governance (minimizing personal data shared with the AI tool, ensuring the AI tool will not engage in unauthorized data sharing with third parties and AI model training with personal data shared with it); keeping technical documentation and records (documenting when and how AI was used during client representation and what information was provided to the AI tool for internal auditing and data control purposes); and maintaining transparency (communicating with the client about the purpose of AI

205. MODEL RULES OF PRO. CONDUCT r. 1.6(c) (A.B.A. 2025).

use during representation, its associated risks and benefits, and obtaining client's informed consent), human oversight (attorney investigation of AI vendor's privacy and cybersecurity measures and enforcement of confidentiality via a confidentiality agreement with an AI vendor); and cybersecurity (ensuring the AI tool has robust AI-specific cybersecurity).

Lawyering tasks accomplished with AI or generative AI tools with minimal or no risk might involve editing grammar and formatting select legal documents (template generation, boilerplate motions, certificates of service), as well as case law summarization, scheduling, and workflow automation, so long as the client's personal data or sensitive information is not used in the process. Under an AIA-like, risk-based assessment system, such uses would not necessitate additional protective measures. Nevertheless, even where the AI risk-based assessment does not require attorneys to take additional data protection and privacy measures, Rule 1.6's original confidentiality and data security provisions would still apply.

Because the AIA and GDPR are intended to work in concert with each other to protect an individual's personal data and privacy rights, the A.B.A. should also amend Rule 1.6 to incorporate certain GDPR protections. The data protections mandated in the AIA and GDPR overlap in some areas. Thus, the GDPR's protections not offered in a categorized AI risk-based assessment modeled after the AIA ought to be added to the rule's comments as well to ensure comprehensive safeguards preserve a client's privacy and confidential information. Specifically, key GDPR principles absent from an AIA risk-based categorization include data minimization practices (data that is collected and used by an entity is limited to only what is necessary to accomplish a task) and data processing or purpose limitations (data is only used for the specific task or process it was collected for—forbidding unauthorized data sharing with third parties). For purposes of this proposal, these key principles are included in the discussion above with the requirements triggered by an attorney's use of AI in the high-risk category.

Importantly, while the proposed changes to Rule 1.6 provide greater protection for a client's privacy and personal data in the age of artificial intelligence, attorneys should still "be mindful . . . that

compliance with minimum standards of any kind—including those delineated in ethics rules—should only be a starting point for effective [privacy and data protection]."[206] In short, attorneys should consider voluntarily adhering to some or all of the requirements in the high-risk category even when their AI use would not obligate them to do so.

B. Counterarguments

The legal profession is confronting unprecedented challenges with the advent of the AI revolution and its transformation of core lawyering tasks and skills. Arguably, the Model Rules may be nimble enough to address the complex privacy and data protection issues associated with using AI since the rules are written vaguely and intentionally, in order to allow attorneys and their ethical obligations to evolve as the technology does.[207] However, this contention rings hollow in light of AI's unique and powerful nature and the significantly more complex risks it presents. In fact, more than a decade ago, the A.B.A. was driven to amend the Model Rules in response to technological advancements that were arguably less monumental than AI and generative AI. Indeed, the A.B.A.'s flurry of recent actions relating to AI and generative AI, as discussed above in section two, underscores that the Model Rules are insufficient in their current form and therefore amendments are necessary.

Critics of the EU's AIA and GDPR lament the constraints that these frameworks place on AI development and data collection, citing fears the regulations may slow innovation and growth in the technology and business sectors. Similar concerns may be raised in response to proposals to amend the Model Rules to account for attorneys' use of AI and generative AI technology for core lawyering tasks, including research, writing, litigation analysis, client intake, and discovery review. However, opposition to using an EU-based approach as a model for Rule 1.6 amendments, grounded in fears that it might slow innovation in the legal profession, is speculative at best. On the contrary, following an EU model—a leading global and cutting-edge standard—would demonstrate the A.B.A.'s commitment to treating

206. Simshaw, *supra* note 77, at 562.

207. Cook & Mavrova Heinrich, *supra* note 11, at 333.

the Model Rules and its ethical obligations as more than just a checkbox exercise. Moreover, "[r]egulatory reform can promote innovation and . . . growth by allowing [attorneys] more freedom to focus their efforts on inventiveness, rather than navigating the overwhelming regulatory road to compliance."[208] Thus, "[e]xplicit national rules for AI implementation will paint a clearer future for AI" in law practice.[209]

VI. Conclusion

The rapid advancement and adoption of AI, specifically generative AI, is reshaping the practice of law, and thus the threats to client privacy and data are reshaping too. However, Model Rule 1.6 remains stagnant despite advancements in AI technology and the legal profession. The A.B.A. should provide attorneys with modernized guidance on how to safeguard client privacy and data when using AI tools. To do so, the A.B.A. should amend the rule and its comments using the EU's AI and data protection regulatory framework as a model. This approach to reshaping the rule for the AI age will create clarity for attorneys about their ethical obligations, build trust in utilizing the technology for both attorneys and clients, and allow for accountability when confidentiality breaches and privacy harms occur during representation.

208. Hillman, *supra* note 21, at 824.

209. *Id.* at 825 (discussing the need for explicit and strong national rules for AI development and use in the U.S. and likening it to the need for strong pharmaceutical regulations, "The FDA regulatory framework applies a similar methodology for developing pharmaceuticals, and the United States, consequently, is a leader in worldwide drug development. . . . AI has the potential to create an even greater impact on society than will drugs, and care should be taken accordingly").