Between a Bot and a Hard Place: Confidentiality and the AI Legal Landscape

By: Julia Feder

TABLE OF CONTENTS

I. Introduction

Artificial Intelligence (AI) use has exploded across the professional world over recent years at a seemingly exponential rate. A report by McKinsey & Company found that 78 percent of surveyed organizations use AI in some business function, up from 72 percent since just early 2024.[1] The spread of AI can almost be looked like a fungus as it reaches into every crevice of modern professional, and personal life. With this rampant AI use, no professions have escaped this integration, including the world of the law.[2] Lawyers are advocates responsible for protecting the information their clients share to ensure they provide effective legal representation.[3] Under the Model Rules of Professional Conduct (Model Rules) Rule 1.6, lawyers generally must safeguard disclosures of information relating to the representation of a client and make reasonable efforts to prevent the inadvertent or unauthorized disclosure of or unauthorized access to information relating to the representation of a client.[4] In the age of AI, law firms and lawyers planning to incorporate AI into their legal work must face the possibility that this use could infringe important legal and ethical rules.

Part I of this article contends that the practice of lawyers inputting confidential client information into AI systems poses significant risks. To mitigate these risks, lawyers must implement reasonable measures for safeguarding this information, which includes ensuring robust data security, understanding the systems in use, and actively advocating for appropriate

[1] *See* Singla et al., *The State of AI: How Organizations are Rewiring to Capture Value*, Quantum Black AI by McKinsey, March 2025, at 14 (finding that this 78 percent is up from 72 percent in early 2024 and 55 percent a year earlier).

[2] *See Artificial Intelligence: What it is and why it matters*, SAS, https://www.sas.com/en_us/insights/analytics/what-is-artificial-intelligence.html (describing how every industry is in high demand for AI's data processing capabilities).

[3] *Rule 1.6 Confidentiality of Information – Comment*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/.

[4] *Rule 1.6 Confidentiality of Information*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/.

legislative protections. Part II of this article will discuss how these AI systems work and how legal AI use implicates Rule 1.6 of the Model Rules. Part III will inform lawyers on how to avoid data breaches of client information and discuss how legislators could assist in this issue. Finally, Part IV will conclude that AI use is an existing issue for confidentiality but can be mitigated with reasonable efforts or precautions by lawyers and appropriate regulatory or legislative oversight.

II. BACKGROUND

A. AI and Use in the Law

1) AI: What Is It and How Does It Work?

The concept of AI was first introduced in 1956 for problem-solving in fields like mathematics, with computers trained to mimic human reasoning.[5] AI learns by making predictions based on large sets of data, or "training data," in which the AI teaches itself to make accurate decisions.[6] AI systems are prediction models that use a specific prompt to evaluate patterns through this training data, looking for other responses deemed helpful based on similar prompts.[7] Training data includes massive amounts of information, to ensure that the AI is making accurate predictions.[8] For example, a dataset may consist of pictures of cats, and through training, the AI will associate similar images with a cat's features.[9] While the AI does not understand what a cat is, it is trained to associate these features with the "cat" label.[10] These chatbots do not actually "think" but instead look for statistical similarities to respond.[11] After

[5] *Artificial Intelligence: What it is and why it matters*, *supra* note 2.

[6] Nayna Jaen, *How AI is trained: the critical role of AI training data*, RWS (Mar. 26, 2024), https://www.rws.com/artificial-intelligence/train-ai-data-services/blog/how-ai-is-trained-the-critical-role-of-ai-training-data/#:~:text=AI%20training%20data%20is%20a,each%20dog%20labelled%20'dog'.

[7] Tim Mucci, *What is Predictive AI?*, IBM (Aug. 12, 2024), https://www.ibm.com/think/topics/predictive-ai.

[8] *Artificial Intelligence: What it is and why it matters*, *supra* note 2.

[9] Jaen, *supra* note 6.

[10] *Id.*

[11] *See* Mucci, *supra* note 7 (explaining how AI reaches conclusions by analyzing thousands of factors and incredibly large sets of data to make predictions).

training, these systems use progressive learning algorithms so that the AI continues training itself on accurate responses, adapting further when fed new data.[12]

Much of the training for these systems occurs before the public uses them to ensure that the user input receives accurate output; however, there are various AI systems that use user data for "system improvement."[13] Some AI chatbots have memory features that can store information about user interactions.[14] While this does not necessarily mean that the system shares one user's data directly with other users, model updates may use this data to formulate accurate future responses.[15] Often, the ability to use this data is agreed upon in the system's terms of service upon signing up, disguised as sharing data to improve their service.[16]

2) How AI is Being Integrated into Legal and Professional Fields

With the growth in scale of the data the AI can process comes the increased integration of these models into various professional fields.[17] When analyzing massive datasets, AIs can automate many repetitive, time-consuming, and manual tasks businesses face.[18] This AI automation is done without fatigue and with highly trained systems that can afford incredible accuracy.[19] The use of AI in business spans any field that could benefit from the automation of

[12] *Artificial Intelligence: What it is and why it matters*, *supra* note 2.
[13] *See* Geoffrey D. Ivnik, *Trust me I'm a legal AI: Addressing Accuracy and Confidentiality Concerns*, LEXISNEXIS (July 17, 2024), https://www.lexisnexis.com/community/insights/legal/b/thought-leadership/posts/trust-me-i-m-a-legal-ai-addressing-accuracy-and-confidentiality-concerns?srsltid=AfmBOop55WoKk6R3zo7POkKzjhJmXoqiQYekjP_m5zuzOrqDomi9B66Y (comparing AI's continual improvement of itself by feeding on new data to the ravenous plant from the "Little Shop of Horrors"); *Will AI share my inputs with other users?*, Grantable (Aug. 7, 2024), https://www.grantable.co/guides/will-ai-share-my-inputs-with-other-users.
[14] *See* David Coher, *Navigating Arbitration Confidentiality Challenges In Age Of AI*, LAW360 (Jan. 28, 2025), https://www.law360.com/articles/2286924/navigating-arbitration-confidentiality-challenges-in-age-of-ai (informing that strict controls must be in place for how information is saved and retrieved by AI).
[15] *See id*. (warning that improved AI personalization means additional memory capabilities).
[16] Ivnik, *supra* note 13.
[17] *Artificial Intelligence: What it is and why it matters*, *supra* note 2.
[18] *Id*.
[19] *See id*. (noting that humans are still essential to set up the system and ask the right questions).

daily tasks or the AI's prediction capabilities.[20] AI's are used in healthcare to analyze X-ray readings, in retail to offer personalized shopping recommendations, in manufacturing to forecast supply and demand, and in finance to identify fraud.[21] In a Thomson Reuters survey of 2,200 professionals and C-level corporate executives from over 50 countries, 77 percent believed that AI's impact on their work will be high or transformational within the next five years.[22] With AI's integration into many professional areas, this use has inevitably seeped into the legal field.

AI use has exploded across the different areas of the legal field and various aspects of legal work. Lawyers may use AI to analyze cases, do legal research, or create templates of documents for court.[23] These AI may be used to streamline the review process, digesting discovery information like documents.[24] Especially for data stored electronically in e-discovery, AI can consolidate and analyze data for a fraction of the effort and cost.[25] In due diligence, lawyers can use AI to cut down on hours of review and quickly draft contracts.[26] A significant concern with lawyers using AI is the system's capability to misappropriate sensitive client information, violating the confidentiality between the lawyer and the client.

[20] *Id*.
[21] *Id*.
[22] *How AI is transforming the legal profession (2025)*, THOMSON REUTERS (Jan. 16, 2025), https://legal.thomsonreuters.com/blog/how-ai-is-transforming-the-legal-profession/.
[23] *See* Davinia Cutajar, *Balancing Efficiency and Privacy: AI's Impact on Legal Confidentiality and Privilege*, INT'L BAR ASS'N (Nov. 29, 2024), https://www.ibanet.org/balancing-efficiency-and-privacy-AI-impact-on-legal-confidentiality-and-privilege (mentioning how reliance on AI can slip into negligence, referencing cases in the U.S. and Canada where lawyers unwittingly submitted fabricated legal precedents generated by AI).
[24] Owen Wolf & Eddy Salcedo, *With AI Use, Lawyers Need to Ponder Confidentiality Stipulations*, BLOOMBERG L. (July 1, 2024, 4:30 AM), https://news.bloomberglaw.com/us-law-week/with-ai-use-lawyers-need-to-ponder-confidentiality-stipulations.
[25] *Id*.
[26] *Id*.

B. *AI and Rule 1.6*

1) *Rule 1.6*

Lawyers are obliged to refrain from revealing client information in breach of confidentiality. Under Rule 1.6(a) of the ABA's Model Rules, lawyers are prohibited from disclosing information related to their representation of a client without the client's informed consent, authorized disclosure for purposes of representation, or permitted disclosure under certain exceptions laid out in the rule.[27] This confidentiality is not limited to matters communicated by the client to the lawyer but instead relates to all information associated with representation from any source.[28] Disclosures from a lawyer are only reasonably likely to reveal this sensitive client information if, from this information, a third party could ascertain the client's identity or the situation surrounding the client's case at issue.[29] This obligation of confidentiality extends beyond the termination of the client-lawyer relationship.[30]

[27] *Rule 1.6 Confidentiality of Information*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/.; Rule 1.6 states that, "A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary:

> (1) to prevent reasonably certain death or substantial bodily harm;
> (2) to prevent the client from committing a crime or fraud that is reasonably certain to result in substantial injury to the financial interests or property of another and in furtherance of which the client has used or is using the lawyer's services;
> (3) to prevent, mitigate, or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services;
> (4) to secure legal advice about the lawyer's compliance with these Rules;
> (5) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;
> (6) to comply with other law or a court order; or
> (7) to detect and resolve conflicts of interest arising from the lawyer's change of employment or from changes in the composition or ownership of a firm, but only if the revealed information would not compromise the attorney-client privilege or otherwise prejudice the client."

[28] *Rule 1.6 Confidentiality of Information – Comment*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/.

[29] *Id*.

[30] *Id*.

Additionally, under Rule 1.6(c) of the ABA's Model Rules, lawyers must make reasonable efforts to prevent any information relating to their representation of the client from inadvertent or unauthorized disclosure or access.[31] Rule 1.6(c) instructs that lawyers are prohibited from disclosures that reveal information but also from any disclosures that could reasonably lead to the discovery of the information by a third party.[32] The competency requirement in Rule 1.6(c) revolves around the need for lawyers to appropriately safeguard client information against third parties by taking **reasonable efforts** to prevent a third party's access or disclosure.[33] Whether a lawyer took these reasonable measures can be determined based on the sensitivity of the client information, how likely the disclosure is without additional safeguards employed, how much those additional safeguards would cost, how difficult the implementation of these safeguards would be, and how much the use of the safeguards would negatively affect the lawyer's representation of clients.[34]

Model Rule 1.6 finds that for virtually transmitted communications involving information about client representation, the lawyers are required to take **reasonable precautions** against unauthorized access to information by unintended parties.[35] Reasonable precautions do not mean special security measures, like encryption or access controls if the communication method that

[31] *Rule 1.6 Confidentiality of Information*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/.

[32] *Id*.

[33] *Rule 1.6 Confidentiality of Information – Comment*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/; *See* Michael Scott Simon & Andrew Pery, *AI and Attorney-Client Privilege: A Brave New World for Lawyers*, ABA (Sept. 5, 2024), https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-september/ai-attorney-client-privilege/ (finding that under Rule 1.1 Competency, lawyers must maintain technological competence and have a "trust but verify" approach to AI that does not compromise accountability).

[34] *Rule 1.6 Confidentiality of Information – Comment*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/.

[35] *Id*.

the information transmits upon affords a reasonable expectation of privacy.[36] As clients have a reasonable expectation of privacy in the confidential information they disclose, and the ABA's Model Rules find that this expectation is reasonable as they developed Rule 1.6, lawyers must not input client information into an AI system that could *possibly* reveal this information in the future.[37] Whether the lawyer reasonably should expect the information to remain confidential depends on how sensitive the information is, and whether the privacy of the way the information is communicated is protected by the law or a confidentiality agreement.[38]

2. AI and Rule 1.6

Rule 1.6 directs lawyers to safeguard confidential client information relating to representation.[39] Confidential client information includes information protected by attorney-client privilege, information that would be embarrassing or detrimental to the client, or any other information the client has asked to remain confidential.[40] Through AI, an attorney that inputs confidential client information into a system that trains itself on inputted queries can violate attorney-client confidentiality as the AI learns from the questions asked.[41] The AI may not directly reveal confidential client data to a third party following the user input; however, the issue lies in the possibility of this disclosure.[42]

[36] *Id.*; *See Expectation of Privacy*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/expectation_of_privacy (describing how a reasonable expectation of privacy involves an individual exhibiting an actual [subjective] expectation of privacy and the expectation is one that society is prepared to recognize as reasonable).
[37] *Rule 1.6 Confidentiality of Information*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/; *Expectation of Privacy*, *supra* note 36.
[38] *Id.*
[39] *Id.*
[40] Richard DeMaio, *Ethics and AI: What Lawyers Need to Know*, Campolo, Middleton & McCormick, LLP (Sept. 16, 2024), https://cmmllp.com/ethics-ai-law-lawyers/.
[41] *Id.*
[42] *Id.*

A lawyer still violates their ethical duties when any AI inputted information has the risk of unauthorized public disclosure. Lawyers who use AI to analyze cases or draft legal documents may expose client information to an AI provider who does not guarantee that the information will not be used to retrain the system.[43] AI cannot differentiate between privileged and non-privileged information.[44] Once this information is integrated into the system's training data, removing one piece of information is nearly impossible without completely retraining it.

As 63 percent of lawyers said they used AI for work in 2024, and 12 percent say they use it regularly for work, the risk of client information being leaked by a lack of reasonable measures or reasonable precautions taken by AI-using lawyers is not a hypothetical.[45] A notable case of unethical AI use by lawyers would be in *Wadsworth v. Walmart Inc.*, in which lawyers representing Walmart used an in-house AI system to upload a brief, before making several inquiries to generate case law that would set forth requirements for a Motion in Limine.[46] The lawyer then used the cases generated in the Motion before submitting them to the court, where they were subsequently discovered.[47] While the unethicality of this use is related to the lawyers' responsibility to do a legal inquiry, it raises questions about whether other attorneys may utilize AI systems to input a client's confidential information to generate a brief and conduct research into similar cases. Additionally, the lawyers who used AI in *Wadsworth* did so on their in-house AI system; unethical use of an open system could allow for the breach of confidential client

[43] *Id*.

[44] Cutajar, *supra* note 23.

[45] *Future of Professionals Report*, THOMSON REUTERS (July 2024), https://www.thomsonreuters.com/content/dam/ewp-m/documents/thomsonreuters/en/pdf/reports/future-of-professionals-report-2024.pdf.

[46] Wadsworth v. Walmart Inc., No. 2:23-CV-118-KHR, 2025 U.S. Dist. LEXIS 36770, at *5-8 (D. Wyo. Feb. 24, 2025).

[47] *See id*. (finding that a lawyers duties remain unchanged in the age of AI).

information. Lawyers must maintain confidentiality obligations while using AI to avoid leaking client data.

III. Analysis

A. AI and Rule 1.6

1) Confidentiality and Data Breach

Lawyers are prohibited from revealing confidential client information, which input into an AI system can present the possibility of a data leak.[48] A lawyer who enters client information into an AI database may violate their ethical obligations to the client.[49] There is a small risk that this information could be publicly disclosed, and it is essential that confidential information does not end up in the hands of third parties.[50] Rule 1.6 does not bend to AI use, and a lawyers responsibilities under 1.6 remain just as strong in the context of new technologies.[51]

If a law firm integrates AI into its operational structure, it must ensure that the information it feeds does not amount to confidential client data. If this information is input into the system, there is a startling reality that other clients or downstream users outside of the firm could gain actual access.[52] Lawyers must take reasonable efforts to prevent access to AI's information and prevent third parties' access or disclosure.[53] If using a public-facing open source system like ChatGPT, the law firm must ensure that they strictly examine the terms and

[48] DeMaio, *supra* note 39.

[49] Michael Scott Simon & Andrew Pery, *AI and Attorney-Client Privilege: A Brave New World for Lawyers*, ABA (Sept. 5, 2024), https://www.americanbar.org/groups/business_law/resources/business-law-today/2024-september/ai-attorney-client-privilege/.

[50] *Id*.

[51] *See id*. (referencing the ABA's Formal Opinion 512, which is focused on three core principles: that lawyers remain fully accountable for all work product, no matter how it is generated; that all existing rules of conduct on lawyers are applicable to AI use in the legal field; and that AI will not be going away anytime soon).

[52] *See* Ivnik, *supra* note 13.

[53] *Id*.; *Rule 1.6 Confidentiality of Information – Comment*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/.

conditions of the AI use agreement to ensure that there is no pretext of shared data to improve the service and altogether avoid inputting any sensitive client information if these terms exist.[54] One solution for law firms would be to remove these secretive clauses from contracts before signage or to ensure that the infrastructure that they are using is secure enough that data does not train a large-scale model with users outside the organization.[55] Law firms using public-facing programs to input client information risk stored inputs and integrations of responses into the model.[56] This risk has not gone unnoticed by financial institutions that have prohibited the use of ChatGPT for work-related tasks.[57] Disclosure of this information could result in the use of data to train the program, possibly sharing the information with a third party if no safeguards are taken against this.[58] Although an AI is not a "person" or "entity" to which information can be shared, this information can still be exposed to third parties on this open system.[59]

Implementing an AI system that operates as a closed system, without sharing information into a more extensive network, could be a solution for law firms that do not want to risk client information.[60] A lawyer may want to input the details of client cases while using an in-house system like that employed by the lawyers in *Wadsworth* to train a more competent system; however, this information must be protected with additional safeguards to avoid having non-privileged parties potentially gain access.[61] A more advanced in-house system that could provide

[54] Wolf et al., *supra* note 24.
[55] *See* Ivnik, *supra* note 13 (pointing out that organizations like LexisNexis have made data security and privacy for customers a priority by opting out of AI monitoring features targets towards confidential customer data).
[56] *Id*.
[57] Wolf et al., *supra* note 24.
[58] *Id*.
[59] *Id*.
[60] *See id*. (explaining that confidential client information is usually given an "attorneys' eyes only" designation or further restricted to review by specific individuals identified in a confidentiality stipulation or protective order).
[61] Wadsworth v. Walmart Inc., No. 2:23-CV-118-KHR, 2025 U.S. Dist. LEXIS 36770, at *5-8 (D. Wyo. Feb. 24, 2025); *See* Cutajar, *supra* note 23 (describing how closed systems allow lawyers to benefit from AI's efficiency without exposing client data to external providers).

nuanced and detailed feedback or research does not trump the prohibitions on lawyers against revealing client information or account for the possibility of that system revealing this information to non-privileged parties uninvolved with the case.[62] Attorneys that even use AI to draft an email containing client information may inadvertently train the system on this data.[63] Lawyers are required to take reasonable precautions to protect their client's information.[64]

Ultimately, AI usage at its core may constitute a breach of confidentiality on a public-facing or in-house system as sharing client information undermines confidentiality, and it is difficult to guarantee the system affords a reasonable expectation of privacy.[65] Additionally, an in-house system is costly to invest in and is challenging to keep secure.[66] Another tool for firms is to take precautions to establish policies or guidelines for employees on how to use the technology without potentially compromising privilege.[67] These guidelines include having employees conduct checks on in-house systems to ensure they are secure and learn more about the technology to understand how their actions affect it.[68] Lawyers could also provide assurances to clients that any document marked as "confidential" will not be input into an AI system.[69]

[62] *See* Cutajar, *supra* note 23 (finding that a better solution than closed systems for confidentiality risks is heightened caution).

[63] *See* Wolf et al., *supra* note 24 (discussing how law oriented AI's digest large batches of information such as emails and chat messages in connection to discovery materials).

[64] *Rule 1.6 Confidentiality of Information*, ABA, https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/.

[65] See *Expectation of Privacy*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/expectation_of_privacy.

[66] *See* Cutajar, *supra* note 23.

[67] *Id*.; *See* Coher, *supra* note 14 (raising two legal entities that have published AI guidelines for employees: the Silicon Valley Arbitration and Mediation Center who published guidelines emphasizing safeguarding confidentiality, mandating disclosure of AI use, ensuring competence in AI utilization, and prohibiting the delegation of decision-making responsibilities to AI systems; and the JAMS Artificial Intelligence Disputes Clause and Rules who published rules for AI disputes, including provisions for producing and inspecting AI systems, mandatory expedited procedures and expansive protective orders).

[68] *See* Cutajar, *supra* note 23.

[69] *See* Wolf et al., *supra* note 23 (describing how the approach to avoid input of any document marked confidential may be impractical given how many e-discovery platforms are incorporating generative AI into their products).

2) The Effect of Regulators and Legislators on Protecting Confidentiality

Regulators could serve as the intermediary between this gap of AI technology and lawyer use.[70] Regulatory bodies like law societies and bar associations could oversee an in-house AI system in which lawyers submit anonymized case information to train a legal AI tool for legal entities to use across the country.[71] This system would require close monitoring for potential leakage of client data and a significant investment in data security measures; however, it would give these organizations access to an AI program that can understand the complexities of law across jurisdictions and legal fields.[72] Integration of a trustworthy AI tool into the legal profession may also benefit clients as their cases get handled by lawyers with less hassle or time.[73] These Regulatory AI models must be published under specific licenses to ensure that they can continue to be refined and improved and to democratize the ability to use these tools.[74]

State legislators may also assist in ensuring confidentiality in the age of AI by requiring lawyers to mandate or disclose any AI use in their work. This would deter lawyers from using AI in a way that could infringe on confidentiality or any other ethical use.[75] U.S. states like Illinois and Texas have put outstanding orders that mandate disclosure of AI use in legal documents.[76] Legislators may be able to look to existing AI regulations on the law both domestically and internationally, like the European Union's AI Act and similar initiatives, for both inspiration and to harmonize AI and confidentiality across different jurisdictions.[77] In an effort to assist lawyers

[70] Joshua Lenon, *Why Lawyers' Duty to Confidentiality Restricts Legal AI Training – And How Regulators Can Step In*, Clio, https://www.clio.com/blog/lawyer-confidentiality-restricts-ai-training/.
[71] *See id*. (discussing the paradox AI use present, as lawyers try to use AI to remain in step with other professional field they are hindered in improving AI models by their inability to share case details).
[72] *Id*.
[73] *Id*.
[74] *Id*.
[75] *See* Cutajar, *supra* note 23
[76] *See id*. (referencing how measures like those taken in Illinois and Texas could serve to protect the sanctity of the courtroom from AI-driven breaches of confidentiality).
[77] *Id*.

with integrating AI into the legal field without undermining professional responsibility, the State Bar of California published an opinion entitled, "Practical Guidance for the Use of Generative Artificial Intelligence in the Practice of Law."[78] This opinion says specifically on confidentiality that lawyers must refrain from revealing client information that is protected from being disclosed without informed consent from the client, and at "every peril to themselves must preserve the secrets of the client."[79] The way that California framed their opinion becomes painfully relevant when contrasting the serious issue of AI misuse with the possibility of lawyers shirking their professional obligations to shave time off work for a client's case. These guidelines could discourage prohibited AI inputs and promote use that uplifts client confidentiality.

IV. CONCLUSION

AI is becoming increasingly relied upon in professional life, and the benefits that AI presents should not be withheld from lawyers should they take the proper measures to integrate this technology correctly. AI poses significant risks to client confidentiality when a lawyer does not take reasonable efforts or precautions under Rule 1.6 to safeguard their client information against downstream exposure from integration into training data. With reasonable efforts or precautions taken to protect their client's confidential information, such as securing in-house systems, denying access to inputs for training purposes, and providing guidelines for employees on use, lawyers may be able to use AI without sacrificing professional responsibilities. Responsible adoption of AI into the legal field would significantly benefit from regulatory oversight. Until that occurs, the burden is on lawyers everywhere to represent their clients to the

[78] Nicole Engler, *Using AI In Legal Work: COPRAC's Tips On Confidentiality And Competence*, BAR ASS'N OF S. F. (May 24, 2024), https://www.sfbar.org/blog/using-ai-in-legal-work-copracs-tips-on-confidentiality-and-competence/.
[79] *Id*.

best of their ability without relying on predictive tools that may harm the same clients they are advocating for.