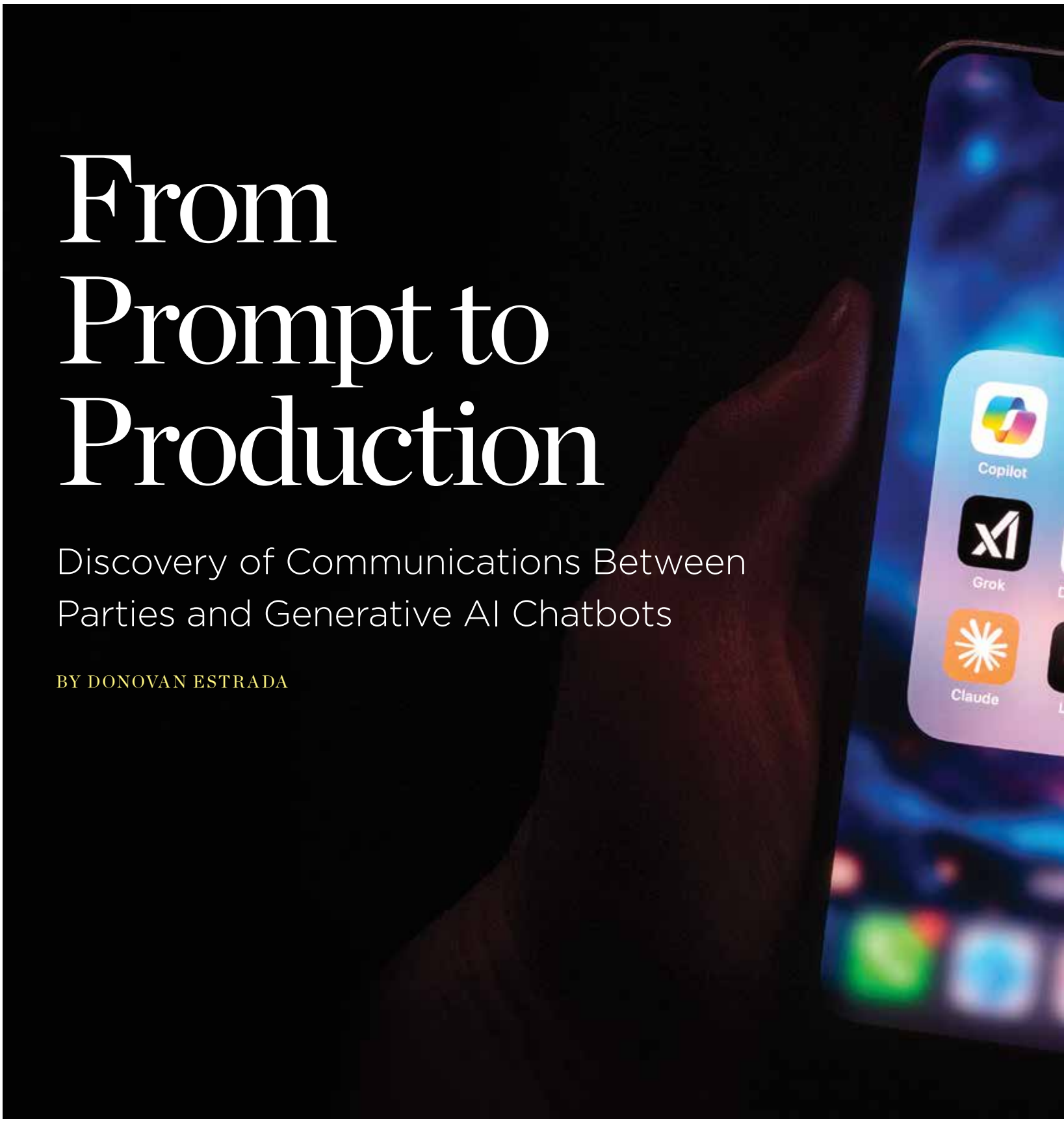

From Prompt to Production

Discovery of Communications Between Parties and Generative AI Chatbots

BY DONOVAN ESTRADA

This article examines how generative AI chat logs may be discoverable in civil litigation, how the Stored Communications Act limits third-party subpoenas, and what Colorado practitioners should know.

The rapid adoption of generative artificial intelligence tools such as chatbots has created new sources of electronically stored information (ESI) that litigators must understand. This is especially true where chatbots such as OpenAI's ChatGPT retain users' prompts and outputs to improve quality and safety. These records may contain facts, strategies, or statements that are relevant and discoverable in litigation.[1] At the same time, the federal Stored Communications Act (SCA) restricts certain service providers from divulging the contents of stored communications.[2] This article explains why the SCA likely prohibits generative AI providers such as OpenAI from being subject to civil subpoenas for the content of subscriber chats, how courts have applied discovery rules to these conversations in other contexts, and what steps lawyers should take to obtain chat transcripts while preserving attorney-client privilege and attorney work product protections.

Overview

Generative AI tools such as ChatGPT have become ubiquitous in both private and professional settings. On one hand, individuals of all walks of life are becoming accustomed to confiding in chatbots for everything from travel planning to psychiatric advice.[3] At the same time, professionals across every sector are finding use cases for generative AI that are completely changing how people work.[4] What very few users may realize is that, unless they opt out, every interaction with their chatbot generates a digital footprint that remains on the provider's servers and is possibly subject to discovery in civil litigation. Fewer users are aware that a recent court order has required OpenAI specifically to preserve all ChatGPT user chats, *regardless* of the user's privacy preferences.[5] As generative AI becomes more commonplace, diligent lawyers must consider the legal implications of this new technology.

Providers of generative AI services face a different dilemma. Clever civil litigants will undoubtedly begin to seek party chat transcripts in discovery, yet the federal SCA may prohibit service providers from divulging users' communications in response to civil a subpoena. Overlay that statutory bar with the Federal Rules of Civil Procedure—and their Colorado counterparts—which obligate parties to produce relevant ESI within their possession, custody, or control, and the legal terrain becomes murky. Navigating these overlapping obligations will be critical for lawyers who must both target generative AI data in discovery and shield clients from inadvertent disclosures in the age of artificial intelligence.

The Stored Communications Act and Generative AI Providers

Congress passed the SCA in 1986 as part of the Electronic Communications Privacy Act. "The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address."[6] The SCA prevents "providers" of communication services from divulging private communications to certain entities and individuals.[7] Specifically, under 18 USC § 2702, providers of an electronic communication service (ECS) or a remote computing service (RCS) generally may not disclose the *contents* of any subscriber communication while it is in electronic storage, except as expressly permitted. The statute lists exceptions for law enforcement subpoenas and warrants but does not create an exception for civil discovery.[8]

The statute distinguishes between an RCS provider and an ECS provider, establishing different standards of care for each.[9] The SCA defines an ECS provider as "any service which

provides to users thereof the ability to send or receive wire or electronic communications."[10] With certain enumerated exceptions, it prohibits an ECS provider from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service."[11] The SCA defines RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system,"[12] and in turn defines an electronic communications system as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications."[13] The SCA prohibits an RCS provider from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service."[14]

Generative AI chat platforms may very well qualify as both ECS providers and RCS providers for purposes of the SCA. They transmit users' prompts and responses over the internet, just as an ECS does, and they retain those interactions to provide a "history" feature and improve the model, which is a form of RCS. Analogously, in *Crispin v. Christian Audigier, Inc.*, the court held that Facebook and MySpace act as an ECS for unopened messages and as an RCS for opened messages and that the SCA therefore bars them from disclosing those messages in response to civil subpoenas.[15] In *Frank v. Gaos*,[16] the plaintiffs brought a class action under the SCA against Google for transmitting their search queries to third-party websites. After multiple dismissal attempts by Google, the case ultimately settled, reflecting the recognition that search queries, like private messages, are treated as the protected "contents" of electronic communications.

Generative AI providers similarly transmit and store communications—albeit with a person and a chatbot—and as a result, courts are likely to conclude that they cannot be compelled to produce chat logs through a civil subpoena; disclosure would require either the user's consent or a criminal warrant, just as the court concluded in *Crispin*.[17] However, the SCA was enacted long before generative AI tools existed, and there is no reported decision squarely addressing whether a one-on-one conversation with a chatbot constitutes a protected "electronic communication." While an analogy can be drawn to social media and internet search providers, only time will tell whether these platforms are covered by the SCA.[18]

> "However, the SCA was enacted long before generative AI tools existed, and there is no reported decision squarely addressing whether a one-on-one conversation with a chatbot constitutes a protected 'electronic communication.'"

Discovery Directed to Parties: *Flagg* and Rule 34

Although the SCA bars civil subpoenas to service providers as described above, it does not insulate parties from their own discovery obligations. In *Flagg v. City of Detroit*,[19] a federal district court addressed whether the SCA shielded defendants from producing text messages stored on a third-party pager service. The court held that the SCA prohibits service providers from complying with civil subpoenas but does not bar discovery directed to the parties themselves.[20] The court explained that parties must produce relevant communications within their "control," which includes the legal right to obtain documents from a third party.[21] Because the City of Detroit contracted with the pager company and could request the messages, it was deemed to have control and was ordered to authorize the release of the messages. Similarly, in *Al Noaimi v. Zaid*,[22] the US District Court for the District of Kansas compelled a litigant to provide consent for his email service provider to release stored emails. The court reasoned that while the SCA bars a subpoena directed at the provider, it does not shield a party from producing communications within their control, which includes the ability to access them or consent to their release.

Colorado Rule of Civil Procedure 34 mirrors its federal counterpart by authorizing a party to serve requests to inspect, copy, or test documents, ESI, and data compilations in the responding party's possession, custody, or control. The rule's definition of ESI is broad and encompasses data that may reside on third-party servers but can be accessed by the party. Applying the same rationale to generative AI conversations as the *Flagg* court did to text messages and the *Zaid* court did to emails, an individual who interacts with a chatbot and can log in to retrieve or export that chat history has possession, custody, or control over the conversations, and any applicable privilege may have been waived. Thus, the SCA may prevent OpenAI or other chatbot providers from responding to a subpoena, but it does not shield the party itself.

CEO of OpenAI Warns of Discoverability of Chatbot Conversations

Sam Altman, the CEO of OpenAI, recently observed that users treat ChatGPT like a ther-

“This sweeping directive highlights how courts may prioritize preservation of potentially relevant evidence over privacy expectations, signaling that generative AI transcripts will be treated no differently than emails or text messages once litigation is underway.”

apist or life coach, sharing deeply personal information despite the absence of doctor–patient or attorney–client confidentiality.[23] Because providers retain chat histories for quality and safety, he cautioned that the conversations could show up as evidence in court and there is little his company could do about it (seemingly without considering the applicability of the SCA). This was likely in reference to *New York Times Co. v. Microsoft*,[24] where Magistrate Judge Ona Wang ordered OpenAI to “preserve and segregate all output log data that would otherwise be deleted on a going forward basis until further order of the Court.”[25] OpenAI argued that compliance would require retention of billions of conversations and would conflict with user expectations that deleted chats would disappear, but the district court judge upheld the order.[26] This sweeping directive highlights how courts may prioritize preservation of potentially relevant evidence over privacy expectations, signaling that generative AI transcripts will be treated no differently than emails or text messages once litigation is underway.

Attorney-Client Privilege and Work Product Concerns

Ironically, in *Tremblay v. OpenAI, Inc.*, OpenAI requested the chat logs of the plaintiffs who sued OpenAI for copyright infringement.[27] In objecting to the requests, the plaintiffs argued that only the prompts and outputs attached to their complaint were discoverable and that additional prompts were protected work product as they were created by their attorneys in anticipation of litigation.[28] The magistrate judge ordered production of all prompts and outputs, reasoning that the requests sought factual data rather than opinion work product. The district court judge later reversed that order, describing it as “a misapplication of law as the ChatGPT prompts were queries crafted by counsel and contain counsel’s mental impressions and opinions about how to interrogate ChatGPT, in an effort to vindicate Plaintiffs’ copyrights against the alleged infringements.”[29] The district judge limited the order to those not protected by the work product doctrine but acknowledged that prompts referenced in the complaint are discoverable due to the waiver of any privilege.[30]

In a similar infringement lawsuit, *Concord Music Group, Inc. v. Anthropic PBC*,[31] the defendants argued they were entitled to discovery of all attorney-generated prompts and outputs because the plaintiffs had placed their AI testing at issue by attaching certain results to the complaint. The plaintiffs countered that only those prompts and outputs actually disclosed in the pleadings were discoverable, and that the remainder remained protected as attorney work product. The court agreed with the plaintiffs, holding that undisclosed AI interactions were shielded by the work product doctrine, but that plaintiffs had waived protection as to the specific prompts and outputs included in their filings. In short, the court rejected the defendants’ broad demand and confined disclosure to the narrow scope of materials actually relied on in the litigation. But, compare that with the Delaware Court of Chancery, which has warned that “[p]roviding Confidential Discovery Material to an open [Generative AI] tool is considered a disclosure to a third party.”[32] Taken together, these cases illustrate that while courts are beginning to extend traditional privilege and work product protections to AI-related materials, those protections are fragile and can be waived.

Practical Guidance for Lawyers

To navigate this evolving landscape, Colorado practitioners should consider the following practice tips:

- **Educate clients** about the discoverability of generative AI chats and the risk of waiving privilege or work product protection. Advise clients to avoid sharing confidential information with public AI platforms and to opt out of data retention whenever possible.
- **Issue litigation hold notices** that cover generative AI tools. Require parties to export and preserve all relevant AI prompts, responses, and account settings. Many platforms allow users to download their chat histories.
- **Serve discovery requests on the opposing party** rather than issue subpoenas to the provider. Request prompts, responses, account settings, and any documentation related to generative AI use that relates to the claims or defenses. Courts are likely to

find these materials within the producing party's control.

- **Anticipate and address objections** regarding privilege and work product. Evaluate whether the producing party has placed the conversation at issue and whether privilege has been waived.
- **Incorporate generative AI data sources** into Colorado Rule 16 ESI conferences and case management orders, specifying search terms, production formats, and cost sharing.
- **Review organizational policies** to ensure that employees using personal accounts cannot inadvertently subject proprietary information to discovery orders.

Conclusion

Lawyers owe clients duties of competence and confidentiality. Colorado's adoption of the duty of technological competence means that attorneys must understand how AI tools store and process data.[33] The Sedona Conference, a nonprofit legal policy research organization whose working groups have shaped e-discovery best practices for decades, and other organizations are developing guidelines on AI and e-discovery. Colorado practitioners would be well-served to track these efforts as the law in this area continues to evolve rapidly. As policies evolve, Colorado courts may refine proportionality standards, privilege rules, and preservation obligations for generative AI data. Practitioners should stay current on these developments and participate in shaping sensible discovery protocols. By educating clients, crafting targeted requests, and respecting privilege, Colorado litigators can obtain necessary evidence while protecting sensitive information. CL

Donovan Estrada is an associate in the Denver office of Hall Booth Smith, P.C., where he focuses his practice on civil and construction defect litigation. He received his JD from Texas Tech University School of Law and has written on the intersection of artificial intelligence and the law, including a prior publication in the *Rutgers Law Record*—destrada@hallboothsmith.com.

Coordinating Editors: Timothy Reynolds, timothy.reynolds@bclplaw.com

NOTES

1. FRCP 34.
2. 18 USC § 2702, Voluntary disclosure of customer communications or records.
3. Slavens, "Smarter Living Through Artificial Intelligence," *Emory Magazine* (Summer 2025), https://bit.ly/3QehqvA.
4. Bick et al., "The Rapid Adoption of Generative AI," Federal Reserve Bank of St. Louis (Sept. 23, 2024), https://www.stlouisfed.org/on-the-economy/2024/sep/rapid-adoption-generative-ai#:~:text=Intensity%20of%20use%20is%20broken,N%3D4682.
5. Order, *In re OpenAI, Inc. Copyright Infringement Litig.*, MDL No. 25-md-3143, 2025 U.S. Dist. LEXIS 97943 (S.D.N.Y. May 13, 2025) (Wang, Mag. J.).
6. *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008) (citing Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 *Geo. Wash. L. Rev.* 1208, 1209–13 (2004)).
7. Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 *Geo. Wash. L. Rev.* 1208 (2004).
8. *In re Subpoena Duces Tecum to AOL, LLC*, 550 F.Supp.2d 606, 608–10 (E.D.Va. 2008) (quashing a civil subpoena because the SCA does not permit disclosure); *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (holding there is no civil discovery exception in § 2702); *O'Grady v. Super. Ct.*, 139 Cal.App. 4th 1423, 1446–48 (Cal.Ct.App. 2006) (concluding civil subpoenas to service providers are unenforceable under the SCA); *Crispin v. Christian Audigier, Inc.*, 717 F.Supp.2d 965, 975–77 (C.D.Cal. 2010) (collecting cases and reiterating that the SCA contains no exception for civil discovery).
9. *Quon*, 529 F.3d at 900.
10. 18 USC § 2510(15).
11. *Id.* § 2702(a)(1), (b).
12. *Id.* § 2711(2).
13. *Id.* § 2510(14).
14. *Id.* § 2702(a)(2).
15. *Crispin*, 717 F.Supp.2d 965.
16. *Frank v. Gaos*, 586 U.S. 485 (2019).
17. *Id.*
18. Hill, "Can Generative AI Prompts Be Used for Evidence?" *ABA J.* (Feb. 1, 2024).
19. *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D.Mich. 2008).
20. *Id.* at 358.
21. *Id.* at 357.
22. *Al Noaimi v. Zaid*, No. 11-1156, 2012 WL 4758048 (D.Kan. Oct. 5, 2012).
23. Perez, "Sam Altman Warns There's No Legal Confidentiality When Using ChatGPT as a Therapist," TechCrunch (July 25, 2025), https://bit.ly/3Q2Cw05.
24. *N.Y. Times Co. v. Microsoft Corp.*, No. 1:23-cv-11195; 2025 U.S. Dist. LEXIS 62442 (S.D.N.Y. Apr. 1, 2025).
25. Order, *In re OpenAI, Inc. Copyright Infringement Litig.*, 2025 U.S. Dist. LEXIS 97943.
26. *Id.*
27. *Tremblay v. OpenAI, Inc.*, No. 23-cv-03223, 2024 U.S. Dist. LEXIS 141362 (N.D.Cal. Aug. 8, 2024). *See also* Austin, "Prompts and Outputs Must Be Produced, Court Rules: eDiscovery Case Law," eDiscovery Today (Dec. 5, 2024), https://ediscoverytoday.com/2024/12/05/prompts-and-outputs-must-be-produced-court-rules-ediscovery-case-law.
28. *Tremblay*, 2024 U.S. Dist. LEXIS 141362.
29. *Id.* at *7–8.
30. *Id.* at *9–10.
31. *Concord Music Grp., Inc. v. Anthropic PBC*, No. 24-cv-03811, 2025 U.S. Dist. LEXIS 99068 (N.D.Cal. May 23, 2025).
32. *Slam Corp. v. Lynk Glob., Inc.*, C.A. No. 2025-0693, 2025 WL 1842381 (Del.Ch. July 2, 2025).
33. To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, and changes in communications and other relevant technologies; engage in continuing study and education; and comply with all applicable continuing legal education requirements. *See* Colo. RPC 1.1, cmts. [8] and [9]. *See also* Colo RPC 1.6, cmts. [18] and [19].