KBA ANNUAL CONVENTION
BEYOND PRECEDENT:
LAW'S NEXT FRONTIER
COVINGTON • JUNE 11-12, 2026

When AI Listens: Confidentiality, Discovery, and Ethical Risks in the AI Era

Lawyers Mutual of Kentucky

SelmanCo

This program has been approved in Kentucky for 1 Ethics credit.

Caroline J. Carter, Laura Cole, Cassie H. Cooper, Lori J. Reed, Editors

Published May 2026

Editor's Note: These *2026 KBA Annual Convention* handbook materials are intended to provide current and accurate information about the subject matter covered. The program materials were compiled for you by volunteer authors and from national legal publications. No representation or warranty is made concerning the application of the legal or other principles discussed by the instructors to any specific fact situation, nor is any prediction made concerning how any particular judge or jury will interpret or apply such principles. The proper interpretation or application of the principles discussed is a matter for the considered judgment of the individual legal practitioner. The faculty and staff of the *2026 KBA Annual Convention* disclaim liability therefor. Attorneys using these materials or information otherwise conveyed during the program, in dealing with a specific legal matter, have a duty to research original and current sources of authority. In addition, opinions expressed by the authors and program presenters in these materials do not reflect the opinions of the Kentucky Bar Association, its Board of Governors, Sections, Committees, or members.

The Kentucky Bar Association would like to give special thanks to the volunteer authors who contributed to these program materials.

I. CONFIDENTIALITY CONCERNS WITH AI

Every Kentucky attorney should be aware of the need for client confidentiality under Kentucky Rule of Professional Conduct Rule 3.130(1.6). Combined with the need to maintain technical competence from comment 8 of the Kentucky Rule of Professional Conduct Rule 3.130(1.1), this means that we are required to be aware of changes in technology used for the practice of law. Artificial intelligence is a technology that is changing rapidly. This session is designed to share some of these changes in the field of AI that potentially affect topics of confidentiality. The two major changes that attorneys need to understand are the confirmation that standard eDiscovery rules apply to AI systems, and that AI systems will soon mine prompts to generate advertisements to present to the AI user.

II. AI DISCUSSIONS ARE SUBJECT TO NORMAL DISCOVERY RULES

Several times in the past few months people have asked me about artificial intelligence and eDiscovery. A recent decision from the Southern District of New York, *U.S. v. Heppner*, brought the topic to the forefront.[1] At one level, the decision was entirely expected. Attorney client privilege (ACP) does not apply to actions that happen before the attorney client relationship is formed. Likewise, actions that are not undertaken at the request of an attorney, especially before there is an attorney client relationship, cannot be protected by the attorney work product (AWP) doctrine. The interesting part of this case was the nature of the actions. In this case, the plaintiff had used the Claude AI system to prepare potential defense strategies after he had received a grand jury subpoena. The plaintiff saved the prompts and responses from Claude, which were seized by the FBI when they executed a search warrant.

We should not be surprised that AI interactions are just as discoverable as any other internet content. In October 2025, the Department of Homeland Security issued its first known judicial subpoena compelling OpenAI to disclose user data and ChatGPT prompts in a case.[2] In that case, the target was an alleged child predator, and DHS had been building their case for years. This is the kind of subpoena that is not as controversial as the administrative subpoenas that DHS has been presenting tech companies to identify people who dissent on public forums like Facebook. According to an article on cleveland.com,[3] Google alone received over 28,000 administrative subpoenas in the first six months of 2025.

[1] *U.S. v. Heppner*, No. 25 Cr. 503 (JSR), 2026 U.S. Dist. LEXIS 32697, 2026 WL 436479 (S.D.N.Y. Feb. 17, 2026).

[2] Guru Baran, "DHS Asks OpenAI To Share Information on ChatGPT Prompts Used By Users," Cyber Security News (Mar. 11, 2026), *available at* https://cybersecuritynews.com/dhs-warrant-openai/.

[3] Editorial Board Roundtable, "Is government use of secretive administrative subpoenas in the AI era an invitation for abuse?", Cleveland.com and *The Plain Dealer* (Feb. 15, 2026), *available at* https://www.cleveland.com/opinion/2026/02/is-government-use-of-secretive-administrative-subpoenas-in-the-ai-era-an-invitation-for-abuse-editorial-board-roundtable.html.

The holding in the *Heppner* case did more than just confirm that AI does not change traditional ACP and AWP protections and limitations. The dicta in footnote 3 suggested that using AI could waive privilege by using Claude due to the AI systems privacy policy. Attorneys need to understand that many of the AI systems not only use prompts and user refinements to responses to train the model, but the chats may be accessed by employees for review. There is no expectation of privacy when using these AI systems, especially if you use the free versions. Some companies may provide additional protection for personal paid versions, but the end user licensing agreements are subject to change and may not provide enough protection that would overcome privilege waivers.

Artificial intelligence systems like ChatGPT and Perplexity generally use end-user prompts and responses to train the public versions of the AI LLMs. Most private versions also permit companies to use employee AI chats and response to improve and refine their private models. AI companies also allow the companies who license their private LLMs to integrate employee AI activities into other systems that can be used to investigate how employees are using the system. OpenAI documents several of these integrations on their site.[4] The main purposes for these integrations are to enable eDiscovery, DLP, and SIEM tools. As lawyers, we understand how the eDiscovery tools would be useful to identify, collect, and deliver evidence needed for legal cases. Many lawyers may not be as aware of the way data loss prevention (DLP) tools can be used to identify and prevent the use of sensitive data in a way that could lead to a data breach or the improper sharing of the sensitive data. An example would be having a tool that would realize a user was trying to upload SSNs or credit card data into the system for analysis. Once that information is added to the system, it could potentially be shared as a response to another employee's prompt. Few attorneys are probably aware of the security information and event management (SIEM) tools that can be used to identify more technical aspects of computer usage and to identify behavior that could result in threats to a company's IT infrastructure. Working in the information security field, I have seen AI systems used to find ways to sneak data out of a company in a way that would not be detected. Employees have asked AI to assist them with ways to bypass company policies, such as to build fake receipts for travel expense fraud. In-house counsel should be aware that their use of AI could be monitored, and client confidentiality could be compromised.

During the 2025 KLU sessions, we shared that a researcher found 130,000 chats from ChatGPT, Claude, and Grok LLMs available on the WayBackMachine (https://web.archive.org/).The researcher was able to query this historical archive to find chats that were reachable without credentials. An article on 404 Media[5] that documented this event indicated that the links to the ChatGPT conversations no longer worked, but the ones for the other systems did. I do not assert that all AI conversations will be this easy to find, but to demonstrate that there may be a low threshold to find historical AI conversations.

---

[4] OpenAI, "OpenAI Compliance Platform for Enterprise Customers," *available at* https://help.openai.com/en/articles/9261474-openai-compliance-platform-for-enterprise-customers.

[5] Joseph Cox, "More than 130,000 Claude, Grok, ChatGPT, and Other LLM Chats Readable on Archive.org," 404 Media (Aug. 7, 2025), *available at* https://www.404media.co/more-than-130-000-claude-grok-chatgpt-and-other-llm-chats-readable-on-archive-org/.

III. HOW CAN YOU TRY TO FLAG ACP AND AWP WHEN USING AI?

Realizing that AI prompts and responses are discoverable and may be read by IT personnel under certain circumstances, I recommend adding specific language in your prompts to give you the best chance at challenging eDiscovery attempts to collect information an attorney intends to be privileged. This probably is not needed for AI systems used only for legal purposes, such as a law firm's professional subscription or implementation of systems like OpenAI's ChatGPT or Microsoft's Copilot. This advice is specifically for in-house counsel for business firms.

For the attorney's prompts, I suggest including "This prompt is made by an attorney and is covered by Attorney Client Privilege. Do not share this prompt or the response generated from the prompt with anyone. The response to this prompt must start and end with the text 'Attorney Client Priviledge'." You may want to include the name of the matter for record keeping purposes.

For any AI use related to a legal matter and that should be considered to be AWP, I suggest using the language "This prompt is made at the request of an attorney [the attorney's name] and is covered by the Attorney Work Product Doctrine. Do not share this prompt or the response generated from the prompt with anyone. The response to this prompt must start and end with the text 'Attorney Work Product'." You may want to include the attorney's name and the name of the matter for record keeping purposes.

IV. USING AI FOR EDISCOVERY

Previous CLE sessions for the KBA mentioned that technology assisted review (TAR) is rudimentary AI and has been used for eDiscovery for decades. Attorneys program the system in a way to scan files for key words so that responsive data is identified, privileged data is flagged, and non-responsive data is ignored. It can take several iterations before the process is reliable. Using traditional TAR tools requires attorneys to be proficient with general IT and with the specific TAR system. This was a micro implementation of an LLM AI system for specific purposes.

Modern AI tools are now available that make eDiscovery easier and no longer require an extensive knowledge of IT. The ABA's *Law Technology Today* microsite explained the capabilities of AI in an article last year.[6] The article summarizes the benefits of using AI for legal document review by calling out the following:

- Efficient eDiscovery: Instead of manually iterating the discovery process like traditional TAR tools, AI automates many of these activities and reduces the time needed to ensure accurate information is retrieved.

[6] Clio, "How AI Enhances Legal Document Review," *Law Technology Today*, ABA.com (Feb. 13, 2025), *available at* https://www.americanbar.org/groups/law_practice/resources/law-technology-today/2025/how-ai-enhances-legal-document-review/#:~:text=Efficient%20eDiscovery:%20AI%20tools%20automate,helping%20lawyers%20prepare%20arguments%20faster.

- Document summaries: AI can summarize the content it reviews. This makes attorneys more efficient.

- Drafting documents: The AI tools can draft the pleadings and statement of facts for the case.

- Translation: Some AI tools can translate documents. This is becoming more important as documents may not be in English. It will reduce or eliminate the cost to translate the documents or need to work with another attorney fluent in the foreign language.

- Building case narratives: The AI tools can summarize the case, giving the attorneys a good start on how to proceed.

V. ADVERTISEMENTS ARE COMING AND MAY EVEN BE HERE

CNN.com announced in January 2026 that ChatGPT will soon start targeting users with advertisements that are based on their conversations.[7] These ads will be sent to users in the free and "Go" level subscribers. The higher tier "Plus" and "Pro" subscribers will not receive ads at this time. The advertisements will be based on the user's chat session and will contain a "sponsored" label, like ads that appear on search engines and social media sites. OpenAI confirmed this with a post on their site on February 8. This post confirmed the CNN article but clarified that this is only a test. The post also explained that past chats will also be factored into the logic to determine which ads will be generated.

Realizing that privacy might be a concern, OpenAI attempted to address this by stating *"During our test, we will not show ads in accounts where the user tells us or we predict that they are under 18, and ads are not eligible to appear near sensitive or regulated topics like health, mental health or politics. We'll expand responsibly as safeguards mature and we learn from this test."* The site also showed how to disable advertisements, which will be active by default. Choosing this option will limit the number of daily interactions with ChatGPT.

Open AI claims the ads will not affect the ChatGPT responses, and that the advertisers will only receive aggregated information about advertisement placement. It should be noted that although the advertisers may not know the details, OpenAI does maintain this information and may use it to train their models and to improve future ad placement.

This session focuses on ChatGPT ads because it was in the news in early 2026. Other LLMs are already using ads or have decided not to do so currently. Perplexity has been placing ads

[7] Clare Duffy, "ChatGPT to start showing users ads based on their conversations," CNN.COM Business Tech (Jan. 16, 2026), *available at* https://www.cnn.com/2026/01/16/tech/chatgpt-ads-openai.

[8] "Testing ads in ChatGPT," OpenAI (Feb. 9, 2026), *available at* https://openai.com/index/testing-ads-in-chatgpt/.

since 2024 but will phase them out in 2026.[9] Microsoft Copilot has been serving ads to users since 2024 and plans to continue doing so.[10] The Tech Buzz reports that Claude will not place ads at this time.[11]

VI. ARTIFICIAL INTELLIGENCE AND SURREPTITIOUS RECORDING

Another feature of AI that has become popular in the past few months is the now ubiquitous recording feature available on most popular video meeting platforms, including Zoom, Microsoft Teams, Google Meet, and Cisco's Webex. All these platforms currently indicate when you join that the session is being recorded, and there is an indicator to show that the site is recording. When asked to disable this feature for a particular meeting, my experience has been that the host will usually comply. You can verify by checking the "recording" indicator, if you know where to look for it. It can be a wonderful tool to record exactly what was said in a meeting or to summarize the meetings for the attendees.

Many people are not aware that many devices exist that perform the recording and summarization features outside of the built-in processes seen in the videoconferencing software. Recording devices with AI features are easily available on sites like Amazon.com. At the time this material was created, a device that could record 500 hours of content on a single charge was available for less than $25. It could identify 190 languages, create a transcript, and summarize the conversations you record. One can use these devices to surreptitiously record any conversation in much the same way one could video record with a separate camera or camcorder. The difference with the AI-assisted recording is the immediate transcription and summarization features. Having served in the U.S. Army's Military Intelligence signals intelligence branch, I always assume my conversations may be recorded. With Kentucky being a one-party consent state, I am concerned that my clients could record conversations that should remain confidential.

VII. WHAT SHOULD WE TELL OUR CLIENTS?

With all the changes and challenges AI is bringing, I think it is important we provide all of our clients with some basic information.

A. Do not use AI for legal matters you plan to bring to an attorney. What you share with AI on your own may be used against you in court.

B. Check the Terms and conditions for any internet system you use to protect your privacy as much as possible. In simple terms, remember that any site that is free or

---

[9] Maxwell Zeff, "Perplexity's Retreat from Ads Signals a Bigger Strategic Shift," WIRED (Feb. 19, 2026), *available at* https://www.wired.com/story/perplexity-ads-shift-search-google/.

[10] "About Ads in Copilot," Microsoft Advertising, *available at* https://help.ads.microsoft.com/#apex/ads/en/60343/0.

[11] The Tech Buzz, "Anthropic pledges Claude stays ad-free as ChatGPT embraces ads," (Feb. 4, 2026), *available at* https://www.techbuzz.ai/articles/anthropic-pledges-claude-stays-ad-free-as-chatgpt-embraces-ads.buzz

gives you a discount to entice you to share information may use that information in a way you do not understand.

C. Do not share legal advice from your attorney with anyone else, unless directed to do so by your attorney. This includes using AI as a way of trying to obtain a second opinion.