ALM | LAW.COM

Legaltech® news

Enhancing Protective Orders To Address Generative AI

By David Kessler and Andrea D'Ambra
April 01, 2024

Artificial Intelligence may be the hottest two words in business right now and that is as true in law, litigation and discovery as well. While there may be more hype than substance at the moment, it is clear that the possibilities of using Generative AI in e-discovery to understand your own documents *and that of your opponents* is tantalizing.

Because your opponent may want to analyze your data using their Generative AI tool, as explained in more detail below, you should consider enhancing your protective orders to ensure such use does not unreasonably expose and unintentionally disseminate your client's confidential information.

Even though the evidence is not yet in that Generative AI currently enhances a party's ability to produce documents by making it faster, cheaper, or more defensible, clients and lawyers need to anticipate that their opponents may use it to analyze documents produced to them in discovery. In other words, a party should assume that their opponents are feeding the documents the party has produced into a Generative AI tool to analyze the party's production.

There is nothing inherently wrong with using emerging technology to attempt to make discovery faster and cheaper. In fact, one could argue, that lawyers are duty bound to look for ways to leverage Generative AI and other new technologies to either make discovery cheaper or to enhance counsel's ability to understand the facts and evidence of their cases.

Moreover, even if lawyers are not obligated to do so, those lawyers who do not take advantage of such tools will quickly find themselves at a competitive disadvantage as compared to their more technologically facile brethren and clients

will naturally migrate to lawyers who do leverage these tools (assuming that they are used well and actually provide measurable benefits).

Clients and lawyers, however, need to anticipate their opponent's use and protect themselves from two possible consequences: (1) inadvertent disclosure of confidential information to unauthorized persons; and (2) the practical inability to delete produced documents at the end of a matter.

The purpose of a confidentiality order is to prohibit parties from disclosing the confidential information they receive in discovery to third parties outside the parameters detailed in the order. Likewise, most protective orders require a party to delete their opponent's documents received in discovery when the case terminates (which is meant to protect the producing party's confidential information from inadvertent use, disclosure, and data breach, as well as to protect the private information of employees and other persons whose information is also sometimes commingled with information relevant to the matter).

Given that these protections are already embedded in most protective orders (and it should be in all), why do parties need to make any changes given the growth of Generative AI? The answer is a combination of "honest mistakes" and the inability to "un-ring the bell."

Generative AI is still new and clients and lawyers are still learning how it works and what these tools do with the data these tools ingest and process. In most cases, a lawyer has no idea how sophisticated their opponent or their opponent's lawyer is regarding the use of Generative AI.

While it may be obvious to many that feeding confidential information into a public Generative AI tool, like ChatGPT, would potentially make that data public and risk it being disclosed to anyone using the tool, do parties and lawyers want to take that risk? Yes, the average protective order's prohibition against disclosing confidential information prohibits the use of such public tools, but that does a party no good if it learns that its opponent used such a tool out of ignorance. You cannot realistically "unring" that bell.

As such, we would recommend including specific provisions prohibiting the use of public Generative AI tools to analyze any confidential information contained in a production. You may also want to require a party to take reasonable steps to ensure that any non-public Generative AI tool used will not disclose information to any other user unrelated to the specific matter. One possible clause could read:

Protected Information shall not be submitted to any *open* Generative AI tool (i.e. ChatGTP) or any substantially similar tool that is available to the public. Providing Protected Information to an *open* tool is considered disclosure to a third party.

Likewise, one of the features of many Generative AI tools is that their algorithms improve and transform based on the information they ingest and the prompts that are used to analyze the document corpus.

For certain tools and in certain configurations, the underlying documents may become a resource that the tool uses to better analyze the next set of documents it ingests and processes. The question is whether these tools can disentangle and delete these documents when a matter ends and the opponent has to certify that it has deleted all an opponent's documents as required under the protective order.

Once again, it does a lawyer no good to learn that their opponent has made an honest mistake and did not realize that its Generative AI tool cannot delete data provided in discovery. Yes, they have violated the protective order, but what is the realistic recourse? It is far better to call out the issue early in the matter and level set everyone's expectations than have to clean up a preventable mess after the fact. One clause that could address this is:

Within ninety (90) days after the last of a Party's case is terminated (including all appeals), or such other time as the Designating Party may agree in writing, the Receiving Party shall use commercially reasonable efforts to either return or destroy all documents, objects and other materials produced, including all reproductions thereof, including but not limited to that given to experts and inside counsel. Counsel responsible for the destruction shall certify to counsel for the Designating Party that all such materials have been destroyed to the extent practical. *Before Receiving Party submits Designating Party's Protected Information to a closed Generative AI tool, Receiving Party shall make reasonably sure that it can delete all produced information from the tool at the close of the Matter. Receiving Party will be responsible for destroying such produced information from such tools at the end of the Matter.*

Of course, it goes without saying that what is good the goose, is good for gander. Before one analyzes their opponent's data (or their client's data) with a brand new shiny Generative AI tool, a lawyer should make sure it can be done in compliance with whatever protective orders are in place (whether Generative AI is explicitly addressed or not) and their own duties of confidentiality and privilege.

Generative AI holds a great deal of promise in the e-discovery space and eventually could help significantly reduce the cost of interrogating not only your opponents' production, but your own data. We just need to use it carefully; protecting the confidentiality of both one's client's and opponents' data.

David Kessler *is a partner at Norton Rose Fulbright and the firm's global head of eDiscovery and information governance and U.S. head of privacy.* **Andrea D'Ambra** *is also a partner at the firm and is its US head of technology and U.S. head of eDiscovery and information governance.*