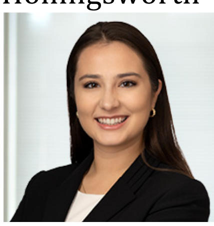
Bloomberg Law

INSIGHT

Counsel's Protective Orders Must Factor in Consistency, AI Usage

Sept. 10, 2026, 4:30 AM EDT

Brett Clements
Hollingsworth



Anna Kutbay
Hollingsworth

Companies and their counsel must craft robust protective orders to guard against improper disclosure of confidential business information and trade secrets.
Photo Illustration: Jonathan Hurtarte/Bloomberg Law; Photo: Getty Images

Parties in litigation face production from sensitive sources while the proliferation of artificial intelligence, privacy issues, and competitive intellectual property demand greater safeguards. Companies and their counsel must craft specific and robust protective orders to guard against improper (and often unnecessary) disclosure of confidential business information and trade secrets.

This is especially important when the same documents may be produced in multiple cases across multiple jurisdictions. Parties also must craft orders with appropriate safeguards for emerging technologies. This includes how to address the increasing use of AI tools — many of which aren't in a closed, protective environment — to summarize and analyze confidential documents. Although it is ideal for the parties to stipulate to an agreed order, counsel may need to move the court for an order to protect a client.

Ensuring consistency in how sensitive documents are produced and used is critical, particularly when they could be subject to production in multiple jurisdictions with different discovery parameters.

Litigants should keep in mind that protective orders benefit all parties: They can shield sensitive information regarding corporate documents and a plaintiff's medical records or personal information from being made public when doing so isn't necessary.

Below are nascent considerations for counsel in drafting and potentially litigating these orders.

Federal-State Interplay

While protective orders entered in federal cases or multidistrict litigations can serve as a potential starting point for document production, corresponding state protective orders in individual cases may differ to comply with local rules, acknowledge prior case-specific agreements with opposing counsel, or otherwise govern the use of documents.

But these state orders should closely track the language of counterpart federal orders to ensure consistent treatment of, often, the same documents. While jurisdictions vary with regard to what is and isn't discoverable, counsel should focus on consistency where possible to maximize protection.

Companies should attempt to use similar or the same language in their state protective orders as they did in similar federal protective orders so scopes align, and vice versa. This also helps ensure the same document productions may be leveraged across cases for efficient, timely discovery.

Failure to maintain sufficient consistency can make obtaining future, favorable protective orders more challenging. For example, the US District Court for the District of Massachusetts in *Bock v. Daimler Trucks N. Am. LLC* denied defendant DTNA's motion for a protective order after it refused to include a sharing provision the plaintiff sought.

The plaintiff used the fact that DTNA had included a sharing provision in a similar protective order in state court to rebut the claim that it would suffer "irreparable competitive harm" if the sharing provision were included. In denying the defendant's motion, the court ordered the parties to submit a revised order including the provision.

AI Safeguards

Because AI use in litigation has become more mainstream, parties should consider including language in a protective order that curbs the ability to upload confidential information into AI platforms that lack appropriate safeguards.

In *Morgan v. V2X, Inc.*, the defendant employer expressed concerns about the pro se plaintiff employee's use of AI for sensitive documents such as insurance policies. The defendant sought amendment to the parties' protective order that would restrict what AI platforms may "process Confidential or Highly Confidential Information."

The US District Court for the District of Colorado found it appropriate to amend the protective order on those grounds. The amendments require that the AI platform refrain from using protected data to train the model; limit third-party disclosures to what's necessary to the service, subject to the same or greater confidentiality protections; and ensure the ability to delete protected data upon request.

Destruction of Data

Although protective orders establish guardrails for the use of sensitive information, parties should set clear timelines for the retention of sensitive and confidential information.

In *Butler v. Daimler Trucks N. Am. LLC*, the defendant argued that the parties' protective order should include a provision requiring the return of confidential information post-litigation. Despite the plaintiff's protests, the US District Court for the District of Kansas agreed with the defendant, finding it "reasonable and supported."

Clauses in protective orders — triggered at settlement or the termination of an action — that mandate the destruction of such materials help maintain the continued confidentiality of information and lessen the possibility of materials being released post-litigation.

Takeaways

Counsel should take care to craft protective orders, including giving due consideration to consistency across parallel matters, risks of improper AI usage, and timely data destruction. Disclosure of confidential information can have severe consequences for clients. For example, public filing of confidential documents can reveal trade secrets or proprietary information to competitors, compromising competitive advantage and opening the door to reputational risks.

Well-drafted protective orders ensure that opposing counsel, parties, experts, and others can't misuse sensitive information without the risk of court-imposed penalties. Using these provisions as tools within complex litigation is paramount for corporate defendants and the counsel defending them.

This article does not necessarily reflect the opinion of Bloomberg Industry Group Inc., the publisher of Bloomberg Law, Bloomberg Tax, and Bloomberg Government, or its owners.

Author Information

Brett F. Clements is a partner at Hollingsworth, where his practice focuses on complex litigation in products liability, toxic tort, and environmental matters.

Anna R. Kutbay is an associate at Hollingsworth, practicing complex litigation defense in products liability and construction and engineering matters.