Reuters Legal News

Navigating the evolving world of e-discovery, information governance and artificial intelligence

By Tara Lawler, Esq., Matthew Hamilton, Esq., Jennifer Mott Williams, Esq., Morgan Lewis

JANUARY 5, 2026

As the new year starts, we explore key areas in e-discovery where companies being informed and consulting the right professionals will be crucial.

Preservation: the essential step you still must prioritize

Companies are rapidly upgrading information technology (IT) systems, including collaborative platforms with ephemeral messaging, and AI-enabled technologies, all of which present challenges for preservation in the event of litigation or regulatory action. These novel sources may auto-delete, version over, or store data in formats requiring specialized workflows. Further, companies' preservation efforts can be compromised by retention policies, custodial misunderstandings, or vendor limitations.

As companies adopt innovative data sources, including AI systems, specific preservation protocols and strategies may be needed. For instance, will the company preserve its AI model training data and prior versions? Will any AI model testing be needed?

Counsel must take an active role in companies' preservation efforts in order to:

- Scope: Define custodians, date ranges, and data types, including non-traditional sources, including ephemeral content and mobile data.
- Update templates: Ensure that legal holds and custodial interview forms include newer data sources, such as AI technologies and AI-generated materials that may be relevant.
- Technical implementation: Ensure that the legal department collaborates with the IT team to suspend auto-deletion and retention jobs, enable legal hold functions, or implement functional equivalents where no native hold exists.
- Education and alignment: Consider providing custodian training to prevent self-help deletion, and align business, IT, human resources, and security teams on preservation objectives. Consider written confirmation of hold implementation.

Data sources in 2026 and beyond

As companies adopt innovative data sources, including AI systems, specific preservation protocols and strategies may be needed. For instance, will the company preserve its AI model training data and prior versions? Will any AI model testing be needed?

Meeting recordings and AI generated transcriptions generate numerous artifacts. Will all artifacts be retained — (e.g., transcripts, attendance reports, summaries, audio summaries, and podcasts generated from the recording) — or just the actual recording? Do you know where that information is stored? Does it differ based upon the type of meeting or who scheduled the meeting?

Such novel data sources merit special attention:

- Threshold assessment: Evaluate whether the new data sources contain relevant information and, if so, determine if preservation and production are proportional.
- Ensure defensibility: Implement standardized and documented processes to establish a clear, verifiable chain of custody.
- Bridge the gap between legal and IT: IT personnel may understand the systems but might not fully grasp the legal obligations and nuances of discovery. It is important to have someone who can translate legal requirements into actionable technical instructions.
- If not proportional, lay out burden: To address the issue of disproportionality in discovery due to increasing

Thomson Reuters is a commercial publisher of content that is general and educational in nature, may not reflect all recent legal developments and may not apply to the specific facts and circumstances of individual transactions and cases. Users should consult with qualified legal counsel before acting on any information published by Thomson Reuters online or in print. Thomson Reuters, its affiliates and their editorial staff are not a law firm, do not represent or advise clients in any matter and are not bound by the professional responsibilities and duties of a legal practitioner. Nothing in this publication should be construed as legal advice or creating an attorney-client relationship. The views expressed in this publication by any contributor are not necessarily those of the publisher.

data volumes, it's important to develop metrics that demonstrate how the undue burden outweighs any potential evidentiary value. This involves quantifying the burden and comparing it to the expected benefits of the discovery process.

Increased requests for mobile devices, messaging apps, and compliance policies

With the proliferation of mobile data, parties increasingly request data related to mobile device usage. Determining whether an organization has possession, custody, or control over mobile device data can be complex.

Key factors include:

- Business use: If the device is used for business purposes, such as accessing company email or applications that are backed up to company systems or whether they have unique data, such as chat or text messages.
- Employer policies: A clear BYOD (Bring Your Own Device) policy that addresses data control and employee obligations is crucial.
- Legal right standard for possession, custody and control: The employer must have a legal right to obtain communications from the device.
- Practical ability standard for possession, custody and control: The employer must have the practical ability to access the data, which can be challenging with modern mobile devices.

> *With the proliferation of mobile data, parties increasingly request data related to mobile device usage. Determining whether an organization has possession, custody, or control over mobile device data can be complex.*

Consider whether your jurisdiction applies the legal right or practical ability standard. Familiarize yourself with your mobile device policies and gain a clear understanding of how custodians are using their devices, not just theoretically. This may include investigating and asking about activities such as texting and the use of third-party applications.

Many organizations are considering establishing information governance programs to manage mobile devices and messaging. These programs often include metrics and risk assessments to evaluate off-channel communications and mobile messaging usage. There is a growing demand for this information to assess possession, custody, or control.

Expanding role of information governance

Proper governance enhances data accessibility, consistency, and trustworthiness. It ensures compliance with data privacy laws, reduces legal penalties, and manages risks related to data breaches and other threats.

It is important that companies have their information governance (IG) in order, which may include:

- Record retention schedules;
- Data disposition policies and procedures;
- AI policies and training;
- Bring Your Own Device policies;
- Legal hold policies and procedures;
- Merger/acquisition/divestiture best practices when appropriate.

Generative AI and written discovery

Understanding your AI policies and practices is crucial when responding to written discovery requests related to generative AI.

> *Proper governance enhances data accessibility, consistency, and trustworthiness.*

Government agencies and parties are updating their definition of "documents" to include AI prompts, conversations, logs, outputs, and decisions. These updates can significantly impact how you collect, review, and produce information.

Generative AI and protective orders

The permissibility of an opposing party using your produced documents to train their private large language model or AI platform depends on the terms outlined in protective orders and other relevant agreements. It is important to carefully review these documents to understand any restrictions or permissions regarding the use of produced materials for AI training.

Rise in AI deep fake evidence

Generative AI deepfakes are making their way into court. With one of the first reported deepfake evidence cases in September in *Mendones v. Cushman Wakefield* (Cal.Super. Sept. 9, 2025), parties should consider the potential generation of fake evidence.

Issues related to metadata (such as atypical fields or copyright information) and internal data characteristics (such as fonts being off, videos glitching, or color scheme changes) may indicate the fabrication of evidence.

Burden breakdown: Persuading the court

Data proliferation is escalating discovery burdens. To support a burden affidavit, be prepared to provide specific details like estimated costs, the volume of documents, and the time required for preservation, collection, and review.

Perform the following to support a claim of undue burden:

- Quantify costs with specific examples for search, collection, and review.
- Detail the volume of documents with evidence rather than unsupported claims.
- Explain the time commitment to complete the discovery.
- Provide evidence — support your claims with evidence.
- Explain why the likely benefit of the requested discovery is outweighed by the burden.
- Discuss the limited relevance and how the discovery is not central to key issues in the case.
- Offer less burdensome alternative sources of similar evidence.

In conclusion, as we navigate the complexities of the new year, staying informed and consulting the right professionals is more crucial than ever. Organizations should continue to prioritize data preservation, especially with evolving IT systems and AI technologies.

Effective information governance is essential to manage mobile devices and messaging, ensuring data accessibility and legal compliance. By implementing robust strategies and fostering collaboration between legal and IT teams, companies can address emerging challenges and mitigate risks associated with data management and AI advancements.

Tara Lawler is a regular contributing columnist on e-discovery for Reuters Legal News and Westlaw Today.

About the authors

Tara Lawler (L), a partner at **Morgan Lewis**, with experience in strategic discovery portfolio management and data governance, focuses on discovery, information governance (IG), data privacy, security, and artificial intelligence (AI). She partners with in-house legal and technology teams to assess, develop and implement best practices for discovery and data management. She is resident in the Philadelphia office and can be reached at tara.lawler@morganlewis.com. **Matthew Hamilton** (C), of counsel at the firm, is a civil litigator and e-discovery counsel with experience representing clients in complex pharmaceutical and medical products liability, data breach, antitrust, and commercial litigation. His practice encompasses all phases of e-discovery, from preservation and collection to cost-effective review and production. He is resident in the Philadelphia office and can be reached at matthew.hamilton@morganlewis.com. **Jennifer Mott Williams** (R), a partner at the firm, helps clients develop and implement efficient ways to manage e-discovery processes and information governance (IG). She provides advice on how to handle the evolving technological landscape, including artificial intelligence (AI), and associated legal obligations. She is resident in Houston and can be reached at jennifer.williams@morganlewis.com.

This article was first published on Reuters Legal News and Westlaw Today on January 5, 2026.