Reuters Legal News

E-discovery and information governance: navigating new challenges and practical tips

By Tara Lawler, Esq., and Matthew Hamilton, Esq., Morgan Lewis

MARCH 26, 2025

The legal and data landscapes are evolving rapidly, particularly in e-discovery and information governance. Legal professionals must anticipate and address these novel challenges in order to best represent their clients and achieve the best possible outcomes.

> *Understanding your client's data landscape — including email environments, communication applications and style, and both unstructured and structured data sources — is crucial.*

To effectively navigate these challenges, one must work closely with clients to understand their data collection capabilities, and pain points, and prioritize collaboration with IT teams to understand the technical aspects and implications of hyperlinks and emojis, among other complex issues. Additionally, strong data privacy and security measures are key, as evolving cybersecurity threats and shifting privacy laws create new risks that must be proactively addressed. As courts rarely excuse parties who struggle to comply with terms they previously agreed to, it is crucial to thoroughly understand a client's technical constraints before finalizing an ESI agreement.

Complex data landscapes and novel data types

Organizations and individuals are generating more data than ever, both in terms of volume and the swift emergence of new types of data. The advent of generative artificial intelligence (AI) coupled with almost universal smartphone adoption has led to an explosion of novel data types. New platforms, applications, and collaborative tools (i.e., unstructured data sources) are rapidly being adopted, leading to complexities in discovery and information governance.

Unstructured data sources present challenges in preserving and collecting relevant information due to their mixed data types and lack of organization. Additionally, the rise in structured data stored in relational databases requires a clear understanding of how to preserve and collect it defensibly.

The complexity of data is further increased by elements like hyperlinks, which may be prevalent due to the overwhelming adoption of cloud platforms. Understanding your client's data landscape — including email environments, communication applications and style, and both unstructured and structured data sources — is crucial.

It is also important to be aware of the client's data preservation and collection methods, capabilities, and policies. If the organization handles its own data collections for discovery, familiarity with their methods and sources is helpful to identify any potential gaps or areas for validation.

Collaboration with the client's IT team is vital to prevent routine data purging and deletion. Engaging with IT staff and platform administrators provides insights into data storage, backup procedures, retention policies, and system changes. This partnership ensures a comprehensive understanding of the client's data landscape and helps identify potential preservation challenges early.

Hyperlinks: What are they?

Document "families" traditionally involved only emails and attachments, making them relatively straightforward in discovery. Consequently, parties often included family production provisions in electronically stored information (ESI) protocols. However, the introduction of hyperlinks requires careful consideration before agreeing to produce entire families or referencing attachments in an ESI protocol.

Hyperlinks are links within emails, instant messages, or other formats that direct users to related documents hosted elsewhere. They often appear in collaborative environments, chat platforms, or email services. Hyperlinks present unique challenges in e-discovery because they are accessed through embedded URLs rather than being part of the email itself. Depending on how a system is configured, hyperlinked documents may not be available at the time of collection, and existing collection tools often struggle to locate them.

Complexities include whether parties must provide metadata for a hyperlinked document, which version is collected (current or at the time of sending), and whether parties must provide documents from hyperlinked files at all.

Parties now often engage in lengthy negotiations and motion practice over whether ESI agreements should include hyperlinked documents. Before negotiating an ESI agreement, assess whether and how your client uses hyperlinks, their ability to collect linked documents, and any related burdens. If hyperlinks are part of your client's data environment, counsel should oversee the collection process to ensure accuracy and completeness. Additionally, understand when your client began using hyperlinks and developed the ability to collect them.

If opposing counsel seeks to include terms about hyperlink handling in the ESI agreement, and you haven't evaluated your client's capabilities, consider using strategic language to delay the agreement until you have more information, if you choose to include it at all.

How to handle emojis

The nature of communications is inevitably changing. While email remains crucial in the workplace and discovery, the use of chat applications like Teams and Slack is increasing. However, preservation and collection features have not kept pace with this rapid adoption. Collaborative channel chats capture conversations, reactions, and exchanges, with participants frequently joining and leaving, creating complex interactive webs.

Emojis present unique challenges as they are nonverbal and can convey various meanings or emotions. Courts have even recognized a thumbs-up emoji as an agreement to a contract. These icons are deeply embedded in our digital communication, both personally and professionally. With the growing presence of emojis in work-related communications, it is important to consider platform-specific variations in emojis, generational differences in emoji interpretations, and context-dependent meanings for emojis.

Effective strategies are needed to ensure emojis are properly identified, collected, interpreted, and produced. Staying informed about technological advancements and leveraging human expertise is crucial for making informed decisions about production. Algorithms are being developed to better understand the nuanced relationship between emojis and text, aiding in interpretation.

ESI agreements — Be mindful of your approach

Some local rules may require court approval for ESI protocols, so you must choose between obtaining a court order or reaching an agreement. Court orders offer clear enforcement but lack flexibility if unexpected issues arise. Recent cases highlight the risks of agreeing to an ESI protocol without fully understanding your client's technical capabilities or the agreement's terms.

Before negotiating an ESI agreement, assess whether and how your client uses hyperlinks, their ability to collect linked documents, and any related burdens.

Courts have little sympathy for parties claiming compliance is impossible after agreeing to specific terms. It is crucial to understand your client's capabilities and pain points before committing to avoid unachievable terms. If an ESI agreement becomes a court order, the court can impose sanctions for noncompliance under Rule 37(b)(2)(A), as it is not limited by Rule 37(e). Overlooking client capabilities and the agreed language in an ESI protocol may lead to sanctions. You may want to consider captioning the agreement as a stipulation rather than an order.

Regardless of your choice, the ESI stipulation or order should include a clause allowing modification or parties to meet and confer if they face compliance challenges. If issues arise, follow this clause and be prepared to show that compliance is unattainable despite your best efforts.

Courts value cooperation. Including a modification or renegotiation clause for unforeseen compliance issues can provide a vital safety net. Demonstrating good-faith efforts to comply is highly valued by courts. This also may weigh in the favor of entering into shorter, more focused ESI agreements based on the information available to the parties.

Data Security, AI, and the protective order

In today's digital landscape, protective orders must evolve if they are to ensure client confidentiality. They should include provisions to prevent data from being uploaded to public-facing AI tools and address risks of inadvertent disclosure. Implementing strong data privacy and security measures is essential due to increasing cybersecurity threats and changing privacy laws.

Protective orders should clearly outline procedures for handling data breaches, including notification and compliance requirements. Additionally, consider amending existing orders to incorporate these provisions and ensure FRE 502(d) language is included, especially if a separate ESI order is not present.

Conclusion

Handling the complexities of e-discovery and information governance requires staying informed and proactive or, failing that, knowing when to engage an expert in the field. Staying updated with new technologies, legal developments, and best practices is crucial for compliance and success.

About the authors

Tara Lawler (L), a partner at **Morgan Lewis**, has more than 20 years of experience in strategic discovery portfolio management and data governance, and helps clients navigate the complex intersection of legal and technical issues, focusing on discovery, information governance (IG), data privacy, security, and artificial intelligence (AI). She routinely partners with clients' in-house legal and technology teams to assess, develop and implement best practices for discovery and data management, aiming to minimize risks, enhance efficiency, and ensure legal compliance. She is resident in the Philadelphia office and can be reached at tara.lawler@morganlewis.com. **Matthew Hamilton** (R), of counsel at the firm, is a civil litigator and eDiscovery counsel with more than 28 years of experience representing clients in complex pharmaceutical and medical products liability, data breach, antitrust, and commercial litigation, with an emphasis on the defense of federal multidistrict litigation (MDL), coordinated state court actions, class actions, and other complex matters. His practice encompasses all phases of eDiscovery, 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.

This article was first published on Reuters Legal News and Westlaw Today on March 26, 2025.