

eDiscovery Case Law Year in Review

2024



TABLE OF CONTENTS

01 Introduction

11 Issues in eDiscovery

13 Report Structure

14 Takeaways from 2024

46 Conclusion

47 Acknowledgments

2024 CASE LAW REPORT

Introduction

Welcome

Welcome to the 2024 Case Law Report from [eDiscovery Assistant!](#)

The pace at which case law on ediscovery issues continues to grow is astronomical, and it shows no signs of letting up. And in the more than 5000 decisions we've seen each year for the last four years, one principle has become very clear—that the rules amended in 2006 and 2015 to provide for the discovery of electronically stored information (“ESI”) *need* to continue to evolve with technology.

Case law in 2024 in particular has started to identify where the rules as amended contemplated technology as it existed in 2006 when email dominated our electronic communications. Social media was still evolving as potential evidence, texting was new, but rudimentary until the iPhone was launched a year in 2007 and didn't grow in popularity for several years, and collaboration platforms including Teams and Slack were not yet founded.

The pandemic and remote work reshaped the landscape of the workforce in the United States and with it, the ways in which we communicate. And, as those methods of communication evolve to how we create, store, send and receive ESI, so too does the evidence that is relevant for litigation. But the rules as amended are merely broad guideposts—think relevance and proportionality—and provide little guidance on the intricacies of how to identify, preserve, collect and produce individual sources of ESI like text messages, Slack messages, hyperlinked files, social media comments, etc. For that guidance, we must look to case law.

And it keeps changing. Two years ago we discussed how courts viewed possession, custody and control in personal mobile devices by employees of a business. Now, the possession, custody and control discussion is largely absent with more of a presumption that if an employee uses a personal device to communicate about relevant matters, that information is discoverable. It's now up to businesses to acknowledge that and plan for it.







The decisions outlined below show some consistent trends that mean that now, more than ever, counsel and their clients need to know what the potential sources of ESI are for the matters that they confront and how to plan for the preservation, collection and production of each separate type of ESI. Video, text messages, instant messaging like WhatsApp and Signal, Teams, Slack, and hyperlinked files are just some of the issues that have to be addressed each time a matter arises. How we ask for ESI is critical to whether our clients can use it effectively.

Our position has always been that despite the volumes of ESI to wade through—with the right planning, there is tremendous power in being able to tell your story faster and more effectively with ESI. As you read through this report, think how you can leverage these rulings to help you tell your client's story. eDiscovery is here to stay—embrace it. Used effectively, ESI and technology allow counsel to do with one person what used to take a team of legal professionals. The opportunity is waiting for you.

The Interplay of eDiscovery Case Law and Litigation Strategy

eDiscovery has evolved over the last ten years as its own substantive area of the law that has added a third job for litigators and the legal professionals that support them. Already tasked with being litigation strategists *and* subject matter experts for a matter, the amendments to the Federal Rules of Civil Procedure and their state equivalents now require litigators to know how to identify and advise clients on preserving each individual source of ESI for a matter, asking for the right form of data by source together with metadata, and thinking about how that data will be authenticated and presented.

Lawyers' obligations now include understanding *the technology* being used to create, store, send and receive evidence—called Sources of ESI—and having an in-depth understanding of the rules regarding ESI to leverage them effectively for their clients. Every time new technologies are introduced, litigators must scramble to understand whether data from those sources is discoverable (hint, yes it is), how to identify and collect it, and what specifics about that data source require negotiation about metadata or other issues in an ESI Protocol. This list highlights just a few of the dozens and dozens of decisions that are key to litigation strategy:

-  What is the story I want to tell and where is the ESI that tells that story?
-  Did the client reasonably anticipate litigation in advance of retaining counsel triggering the duty to preserve?
-  Does my client face any issues for failure to preserve out of the gate?
-  What actions need to be taken to preserve data at the client once the duty to preserve has arisen?
-  What are the specific issues for my case that need to be addressed in an ESI protocol or other agreement to provide and receive data?
-  What metadata fields do I need for each source of ESI?

- Can I redact in my review platform, or does that need to be done before data is loaded?
- What are the acceptable bases for redaction in my jurisdiction?
- Do I have to agree with the other side if I want to redact for non-responsiveness?
- How do I want to present data effectively during a deposition? Attached to motion papers? In a complaint? Typically deponents respond better to seeing data in the format they are used to seeing it in and changing that up can lead to confusion and unclear testimony.
- How will I authenticate the various data sources when it comes to trial? If my IT department screenshots a whole bunch of social media messages from customers, who authenticates them? Will the court allow them? How do I defensibly collect and present social media as part of my story?
- What specific communications are critical to the story I want to tell? Text messages, Slack data, WhatsApp? How will a judge or jury want to see them visually? In what format?
- How can I streamline the review process to focus only on the key issues that matter and avoid expending resources on data that is not relevant?

Case law plays a crucial role in educating litigators and legal professionals on issues like the questions raised above. The analysis and interpretation of court rulings on ediscovery disputes provide lawyers a deeper understanding of how courts and individual judges interpret the rules governing the handling of ESI. This knowledge is critical in helping lawyers navigate a complex and rapidly evolving technological landscape and developing effective strategies for identifying, preserving, and producing electronic evidence. Staying informed about the latest case law developments allows lawyers to ensure that their clients' rights are protected, and that the discovery process is conducted in an efficient, cost-effective, and ethical manner.

The Impact of Generative AI

In last year's report, we identified generative AI as an issue to watch, and it has been the topic du jour *every single day*. In terms of its impact on the ediscovery process, we are starting to see tools in the market leveraging the power of generative AI to assist in document review and summarizing data (think depositions, meeting notes, case law) that offer significant value to litigators by reducing the time spent on mundane tasks. But the more recent models of Generative AI are increasingly better at reasoning—and that opens up many new possibilities for legal to leverage the technology.



2024 and Generative AI has upped the ante again in terms of new complexities with data as evidence, now raising the question of whether prompts or questions asked of these models that generate the results can be discoverable. That will be an issue to watch.

Generative AI is center stage, requiring litigators to know the language of large language models (LLMs) and how those models acquire data. Recent disputes arguing copyright infringement against Meta, OpenAI and Microsoft, have involved requests for discovery of the data used to train the LLMs—issuing an entirely new conundrum for parties responding to those requests.

Issues in Gen AI finally bubbled up into ediscovery case law in 2024 and [seven decisions are now tagged with Generative AI](#) in eDiscovery Assistant from 2024, more than a [dozen overall](#).

Key Themes in Case Law and Why They Matter

Three themes continue to emerge from ediscovery case law, and if you follow the [Case of the Week series](#) hosted by eDiscovery Assistant CEO Kelly Twigger, these will certainly sound familiar:

-  **Plan, plan, plan.** Early planning saves time and money, gives you more time to create a strategy and reduces risk in spoliation or simply not asking for the right evidence. Start thinking about ediscovery for a matter as soon as you know about it or even before you have a matter. eDiscovery preservation and identification issues need to be considered during the very first meeting about a matter. While that timing is usually devoted to the best approach from a legal strategy perspective, ediscovery is a critical part of that early strategy. Planning prior to matters arising, i.e. compiling a data map, identifying liaisons to various departments with key sources of ESI, and understanding the totality of the decisions that need to be made for each type of matter will put you in the driver's seat out of the gate. This theme makes the case for keeping a simple data map up to date, and ensuring that legal, IT and the business are regularly discussing the new sources of ESI being implemented for a client.
-  **Document, document, document.** The reality is that two years from the day you make a decision not to include a custodian, the other side will ask for that custodian and you'll have to defend your decision making process. Write it all down. Use a spreadsheet with tabs – anything basic that lets you track all the discovery elements for a case. Track the legal hold list, process and timing, each individual discovery request and the investigation undertaken to respond to it, etc. We revisit these trackers hundreds of times each case. There are too many details to remember – write it all down. It saves time and money when you have to recreate what happened later during motion practice.

Have Specific Facts to Backup Your Argument. Discovery motions are about the specific facts of your case, and you have to include them in your motion. Counsel’s arguments that review will be costly, or run into the millions of dollars, or can’t be done, will not work without FACTS to back them up. We’ve seen that time and again in the case law where courts deny arguments attempting to limit discovery based on proportionality because counsel provided no specific facts on which to base their argument. You need numbers when talking about costs or volume of documents, an analysis or expert testimony as to why collection of documents at hyperlinks is not technologically feasible, or when the settings were changed on the mobile device to delete text messages every 30 days.

Inherent in each of these themes is the need to understand the underlying technology to allow counsel to make these key strategic decisions. Despite the fact that every case involves ESI, advancements in ediscovery technology, and heightened risks for missteps, lawyers often remain disengaged from the technical side of discovery, creating a costly “disconnect” between data handling and legal strategy.

This gap stems from handing off critical decisions to litigation support or vendors who lack a clear understanding of case objectives, leading to missed opportunities, wasted resources, and suboptimal presentation of evidence. As data sources become ever more complex—including text messages, social media, and AI-generated content—attorneys must proactively shape how ESI is preserved, collected, and presented. By focusing on the ultimate story they need to tell, asking the right questions up front, working collaboratively to educate litigation support professionals on their matter, and leveraging modern ediscovery tools and resources, lawyers can close the gap, streamline discovery, and protect their clients’ interests.

Distribution of Case Law in 2024

2024 saw a 22% increase in the number of civil cases filed in the United States District Courts.¹ With that increase, we expect to see a sharp rise in the number of discovery decisions in 2025 as those cases move further into fact discovery. This year's number of ediscovery decisions at 5091 remained relatively constant with 2023's number of 5209, but with a host of new issues and complexities discussed in detail below. The number of decisions this year represents a staggering number for counsel to keep track of in any size firm, and is further indicative of the continuing evolution of case law in this arena.

Chart 1 shows the rise in the number of decisions in ediscovery since 2015 when the Federal Rules of Civil Procedure were amended a second time to address issues in ediscovery.

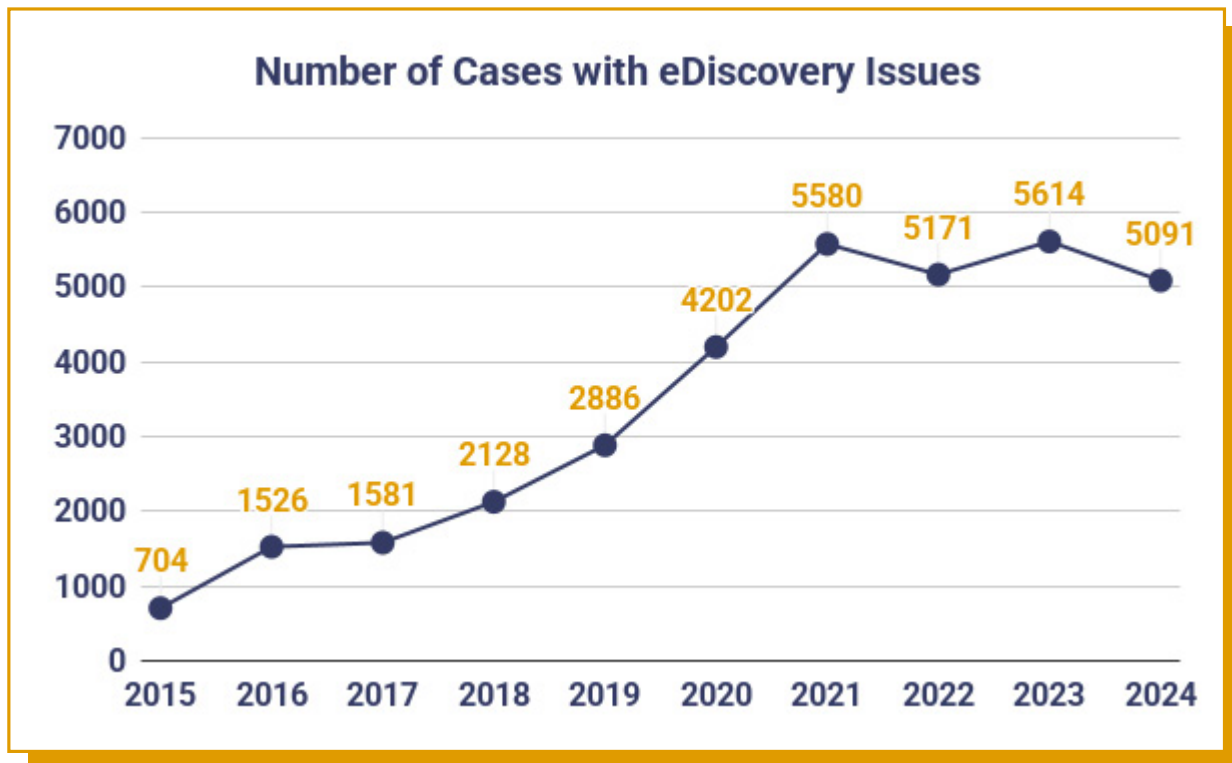
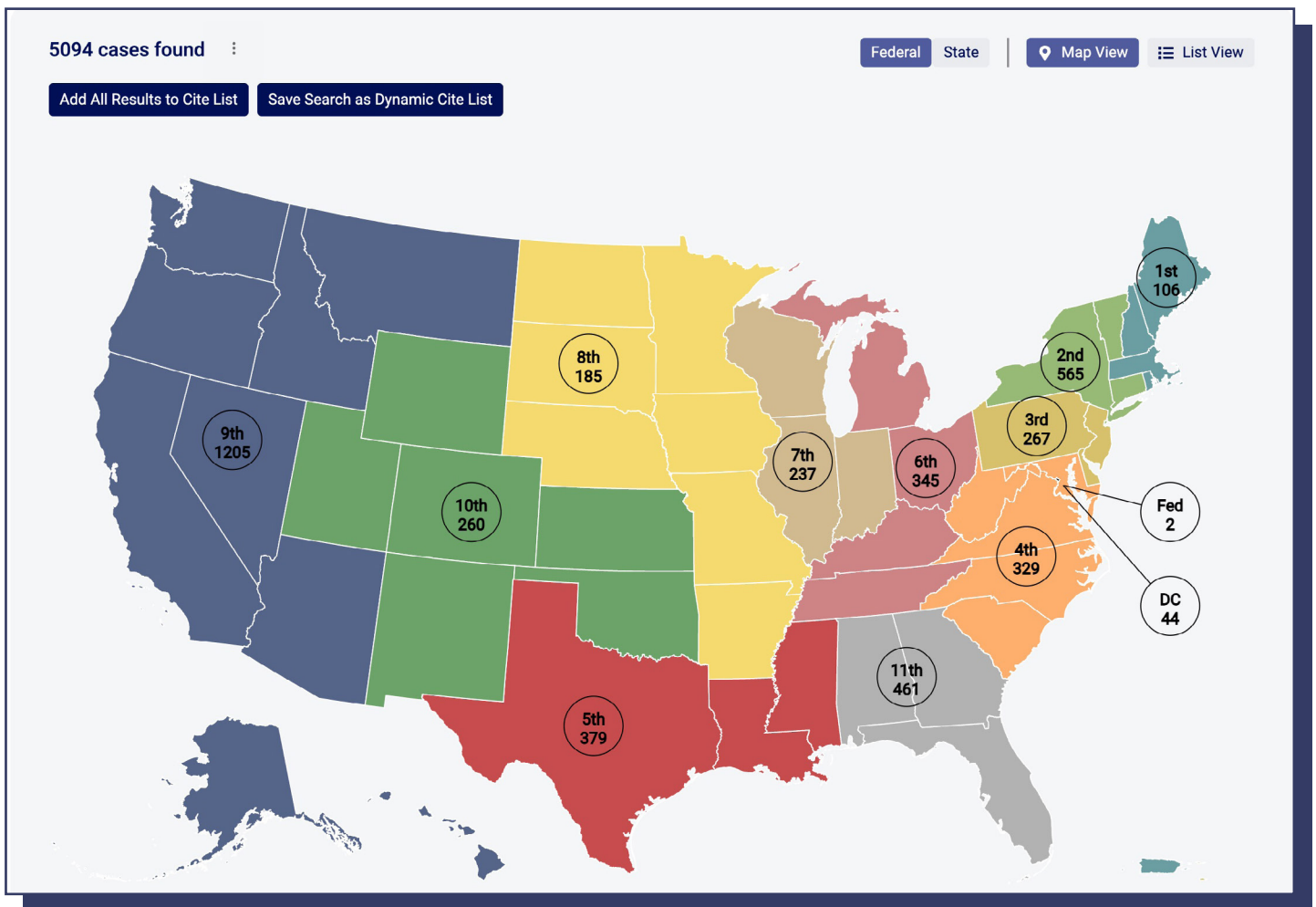


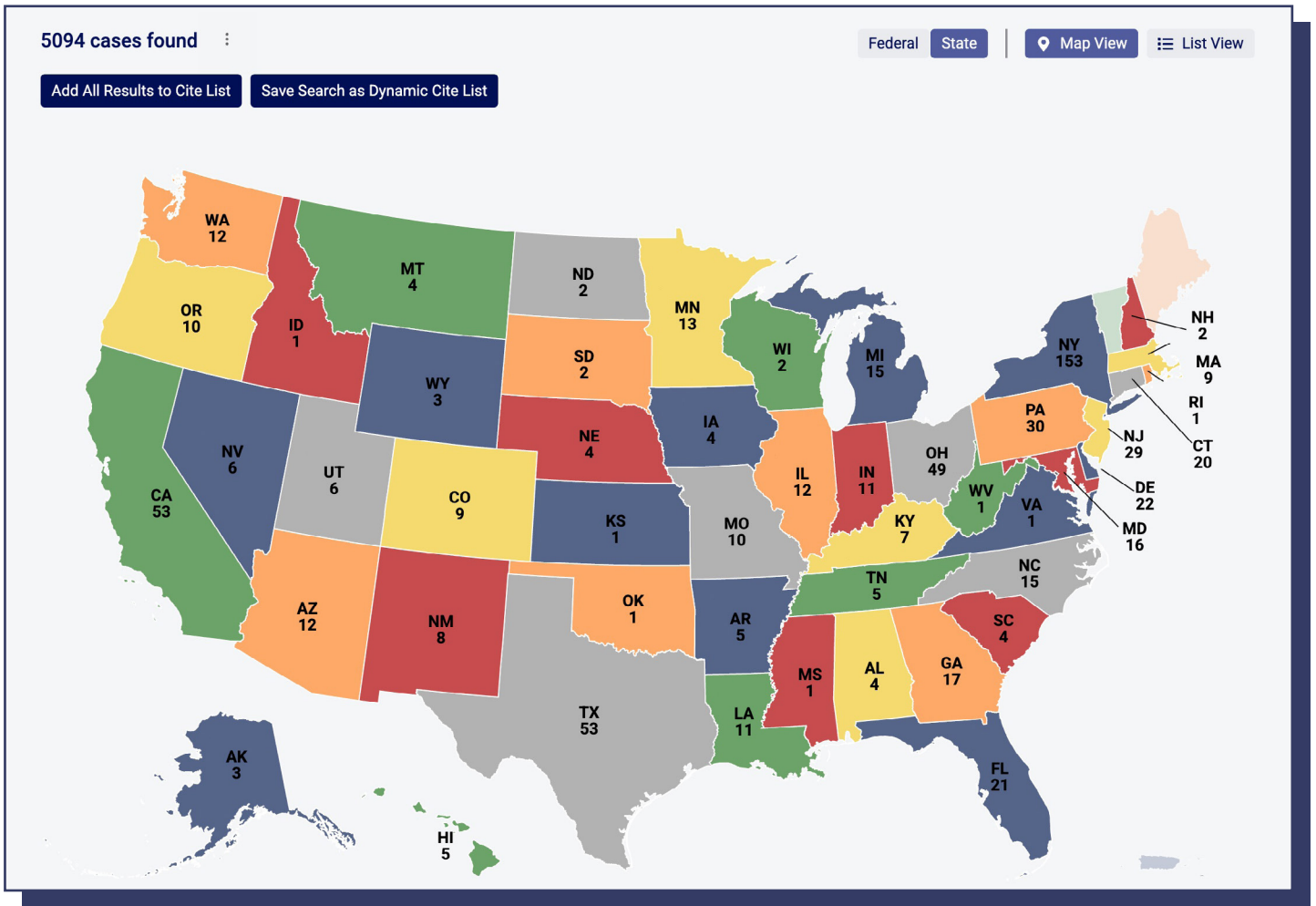
Chart 1 - Number of eDiscovery Decisions since 2015

¹ <https://www.uscourts.gov/data-news/reports/statistical-reports/federal-judicial-caseload-statistics/federal-judicial-caseload-statistics-2024>

Maps 1 and 2 from eDiscovery Assistant show the breakdown of decisions across the federal and state courts in 2024. Users of the platform can click directly into those maps in the application, or drill down to individual district courts using the Jurisdiction filter. Non-users of the platform can view the public links of any decisions included in this Report.



Map 1—Federal Decisions in 2024



Map 2—State Decisions in 2024

Issues in eDiscovery

One of the greatest challenges in staying abreast of developments in ediscovery case law is the wide range of issues on which courts are constantly making decisions based on a specific set of facts. Combined with the reality that no two courts use the same language to discuss an issue (think proportionality, failure to produce, form of production or manner of production), we sought to solve that by creating a proprietary issue tagging structure of [more than 90 ediscovery and technology specific issues](#) to allow users to drill into case law without having to discern appropriate search terms.

eDiscovery Assistant reviews each decision from federal, state and administrative courts for inclusion in our database and then tags each decision with issues analyzed in the ruling. Users can leverage the Issues Dashboard for a description of each issue tag and related tags that may be useful in focusing your search. Issues can be combined to narrow a search, e.g. “Failure to Preserve AND Slack” or “Social media AND authentication NOT criminal” to narrow results to decisions including both issues.

Chart 2 below shows the top forty issue tags in the eDiscovery Assistant platform for 2024.

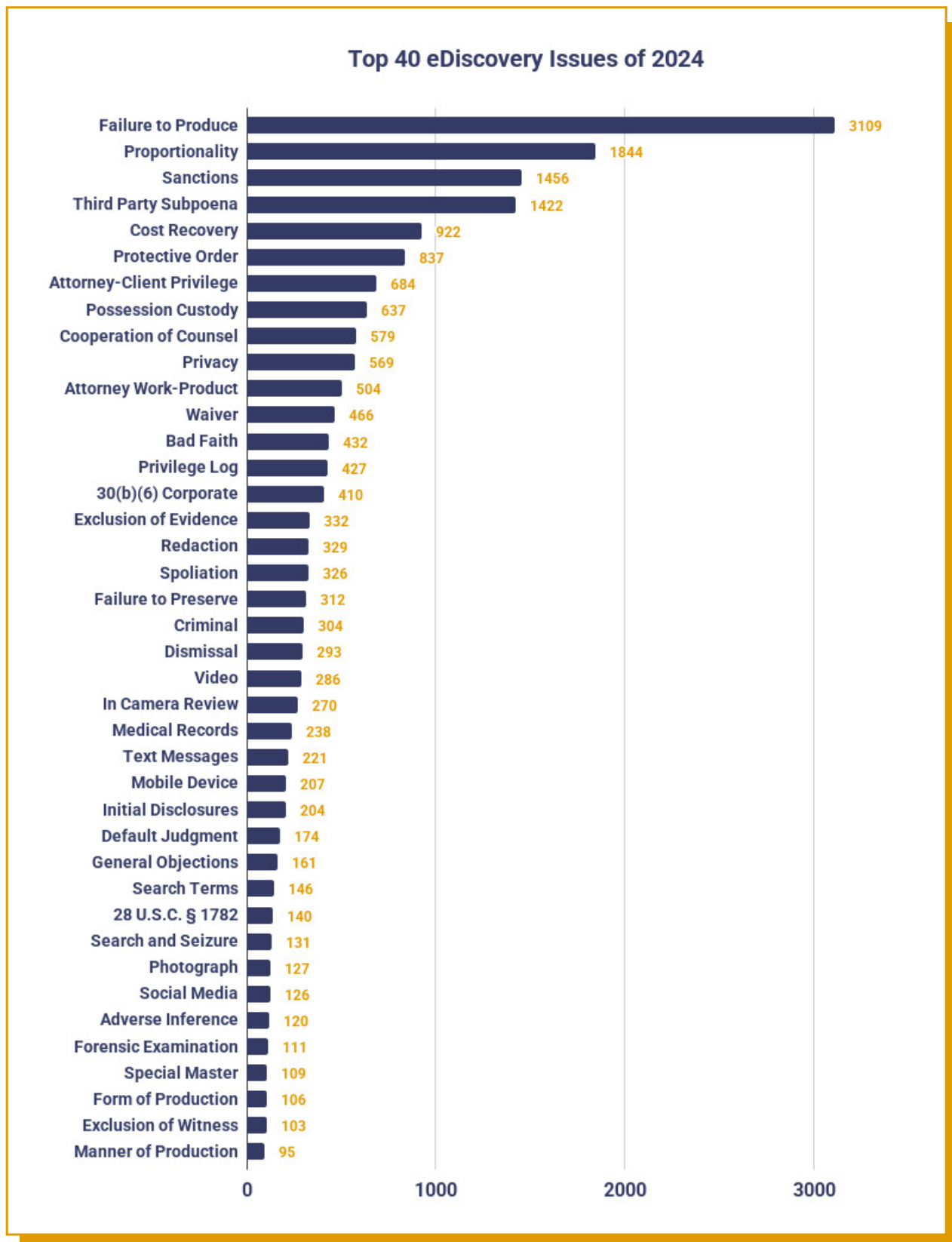


Chart 2 - Top 40 eDiscovery Issues of 2024

Report Structure

This year our report does a deeper dive into more of the issues raised by case law than in years past. The nuanced decisions on important issues that litigators face every day demanded that we include them for you to leverage. Our takeaways from 2024 breaks down the case law and the lessons learned into several subheadings of content, including mobile devices and hyperlinked files, as well as a myriad of other key issues.

If you are familiar with our [Case of the Week](#) series hosted by our CEO Kelly Twigger, you know that Takeaways are the practical lessons learned from each decision and how to adjust your strategy based on the court's interpretation or ruling.

We have also partnered with select software companies and service providers with specialized knowledge of the issues covered to provide insights from the trenches on how rulings affect their everyday work for clients. You'll see quotes from those partners throughout the Report. Page 47 of the report provides an overview of our partners technology or service offerings as well as a link to find out more information.

TAKEAWAYS FROM 2024



Hyperlinked Files in eDiscovery: Legal and Technological Considerations, Case Law, and the Current Landscape

Hyperlinked files have emerged as a significant challenge in ediscovery—not because hyperlinks are new, but because the way we use them and the pace at which we use them has fundamentally changed. In the past, email attachments were static, self-contained files. Today, however, emails often contain links to collaborative platforms (such as OneDrive, Google Drive, or SharePoint) where the “file” is really a living document.

Unlike traditional attachments that remain immutable once sent, these hyperlinked files can be modified, deleted, or even lost if not properly preserved. This fluidity creates uncertainty over whether these linked documents should be treated as part of the original email’s record, complicating both preservation and production in litigation.

Overriding Issues

At the heart of the problem is the contrast between static attachments and dynamic hyperlinked files. With traditional attachments, the parent-child relationship between the email and its attachment is clear: the file is embedded and its version is fixed at the time of transmission. Hyperlinked files, by contrast, reside on external platforms where changes can occur after the email is sent. This raises several key issues:

-  **Preservation:** Courts and practitioners must decide whether—and how—to preserve the “as-sent” version of a document, knowing that the live file may have been altered or removed.
-  **Custody and Control:** Hyperlinked files might not reside in the custodian’s traditional data store; they could be held by third parties or across multiple cloud environments. As a result, the conventional notion

of custodian-based preservation may be insufficient in identifying and accessing relevant documents.

Metadata: Where the parent/child relationship can be provided for in metadata with traditional attachments, no such metadata exists and parties are left to try and find a technological solution to show relationships between emails and hyperlinked files.

Proportionality and Burden: Requesting parties need to balance the relevance of a hyperlinked file against the significant technological and financial burdens that may come with producing large volumes of data from disparate sources.

Currently, the question of whether the technology exists to address this issue and all of its facets depends both on the platform creating the hyperlinked files, and the tools being used to collect them. Parties need to understand both the technology housing the data, and be prepared to discuss their ability to identify and collect data from that technology specifically, together with any limitations that may exist. That is the minimum information counsel should have before negotiating any kind of protocol for a matter involving hyperlinks. To do so before you know can lead you down a rabbit hole as in the *In re Stub Hub* Litigation matter discussed below.

Case Law on Hyperlinked Files

From a legal perspective, the courts have increasingly grappled with how to treat hyperlinked files. Several notable cases illustrate the evolving approach:

- [Nichols v. Noom Inc.](#) (2021): In this early case on the issue, the Court held that hyperlinked files *are not attachments*. The parties' initial agreement on the scope of production was given significant weight, meaning that Noom was not forced to produce additional documents beyond what was initially agreed upon, even after it became clear that Noom had hundreds more documents at hyperlinks than the parties originally contemplated.
- [In re Google RTB Consumer Privacy Litig.](#): This decision underscored that when specific documents at hyperlinks are identified, the requesting party may be entitled to have those documents produced. Here, precision in identifying which hyperlinked files are relevant is crucial, and the parties followed an approach of identifying documents at hyperlinks to be produced twenty documents at a time. This case is a great example of acknowledgement of the issue, and finding a workable solution that provides proportional discovery.
- [In re StubHub Refund Litig.](#): Two decisions from the StubHub litigation reflect the tension between technological feasibility and legal obligation. Initially, [StubHub was required to produce documents linked in emails](#) after agreeing to it in the parties' ESI protocol. Later, after StubHub demonstrated the extreme difficulty and high cost of retrieving contemporaneous versions from cloud applications, [the Court allowed for a modified approach](#) based on "good cause" language in the ESI protocol to amend the production obligations. The lesson from StubHub is twofold—make sure you test the technological capabilities to capture hyperlinked files before agreeing to them in a protocol, and always include the "good cause" language to allow for a "get out of jail free card".

In re Uber Techs., Inc. Passenger Sexual Assault Litig.: Perhaps the most instructive ruling to date, Magistrate Judge Cisneros emphasized that if a party chooses to use a particular storage solution (in this case, Google Vault), then it must provide production of associated hyperlinked files—including metadata that clearly ties the email to the document. The decision stressed that arguments about technological difficulty must be supported by expert evidence and early testing; the duty to preserve begins as soon as litigation is anticipated. Judge Cisneros’ ruling took expert testimony into account and pushed the parties to provide specifics on the technology available, but also held Uber to production knowing it had chosen the tools it did.

UAB “Planner5D” v. Meta Platforms, Inc.: In this case, Meta Platforms successfully argued that retrieving hyperlinked files was overly burdensome. However, the decision also revealed a tension: if the requesting party can review the available data and determine it is nonresponsive, then a blanket burden argument may not be sufficient to avoid production entirely. The UAB case is a bit of an outlier in the hyperlinked files case law progression—in part because unlike other courts, Meta successfully argued it did not have the technological capabilities to provide the hyperlinked documents. But at the same time, Meta argued it had reviewed them all and they were not relevant—begging the question of if you were able to review them, why can you not collect them?

The case law as a whole refuses to define the obligations of a party relative to hyperlinked files until the court understands—through expert testimony generally—what a party’s capabilities are to provide that information in discovery, the relevance of that data and whether the effort and cost to provide it is proportional to the needs of the case.

Technological Considerations

On the technology side, the challenge of hyperlinked files is twofold:




- 1. Dynamic Nature of Data:** Unlike static files, the current version of a hyperlinked document may not reflect the version originally referenced in the email. Preservation tools—such as Microsoft Purview for Office 365 or specialized solutions offered by vendors like Metaspike and Lighthouse—are now being developed to capture “as-sent” versions. Yet, these tools depend on proactive retention policies. If a legal hold is only imposed after a dispute arises, much of the historic data may have already changed or vanished.
- 2. API Volatility and Integration Issues:** Providers such as Google and Microsoft continuously update their APIs for functionality, often without considering the implications for ediscovery. This means that the technical ability to extract and link metadata from hyperlinked files is in constant flux, requiring ongoing collaboration between legal teams and IT experts. The evolving nature of these platforms has led to a rethinking of the “custodian” concept in discovery—from a focus on individual users to a more data-centric approach that considers the various sources and repositories where documents might reside.

“Hyperlinked files are the perfect example of when and why coordination is necessary between counsel and litigation support. The technological complexities of files at hyperlinks—whether we can collect the documents at all, where they are stored, whether contemporaneous versions are possible, or whether metadata is required to identify the relationship between documents—must be considered at the outset for both producing and receiving parties in litigation so that data can be handled effectively to allow parties to leverage it. This is an area of technological complexity where counsel can find themselves in hot water trying to satisfy an agreed upon order when their available technology doesn’t allow for it.”

– Doug Austin
Editor, eDiscovery Today

Where We Stand and Looking Ahead

Right now, the case law and technological landscape suggest that hyperlinked files—when relevant and responsive—should be produced much like traditional attachments. However, achieving this in practice is far from straightforward:

-  **Early Planning and Testing:** Best practices call for an early, proactive strategy that involves both legal and technical experts. Practitioners must test their data collection methods well before litigation escalates, ensuring that retention policies are in place and that the appropriate tools are deployed.
-  **Tailored Protocols:** There is no one-size-fits-all solution. Parties are advised to negotiate protocols during the meet-and-confer phase that specify, for example, incremental production (as seen in the Tesla-related decisions) and the required metadata fields to establish the email–document relationship.
-  **Evolving Expectations:** While recent rulings (especially *In re Uber Techs.*) have moved toward requiring production of hyperlinked files when feasible, courts have also acknowledged the technological challenges involved. Over the next year, as vendors refine their tools and platforms—such as anticipated enhancements in Microsoft’s preservation capabilities—the legal expectations may become more standardized.

Hyperlinked files present a “modern attachment” challenge where the interplay of legal duty, technological capacity, and proportionality becomes critical. The case law—from *Nichols* and *In re Google RTB* to *StubHub*, *Uber*, and *Planner5D*—offers valuable guidance, yet emphasizes that early, informed planning is essential. As the technology evolves, so too will the strategies for managing, preserving, and producing these dynamic documents in litigation.

Mobile Device Discovery

For the sixth year in a row, we saw [more than 200 disputes](#) in 2024 over discovery from mobile devices in matters. This year's case law, however, identified new considerations with respect to obligations in the discovery of data from mobile devices, and specifically text messages—that individual parties are held to the same standards for preserving and producing documents as more sophisticated parties, and the introduction of denial of summary judgment and awarding costs on that motion as sanctions for the failure to preserve under Rule 37(e)(1).

The case law below covers a range of issues that came up this year including additional sanctions for failure to preserve text messages including the denial of summary judgment where prejudice is found under Rule 37(e)(1), preservation obligations in ephemeral data, whether text messages can be redacted for non-responsiveness, and the need to retake possession of company mobile devices when an employee leaves. These issues are just the tip of complexity we saw in mobile device data last year—you'll want to keep your eyes open in 2025.

Failure to Preserve Text Messages

This year saw multiple decisions for the failure to preserve text messages, drawing attention to the need for counsel to actively manage the preservation and collection of text messages vs. relying on their clients to follow their advice.

In [Safelite v. Lockridge](#), the Court found that an *individual defendant* was subject to the same obligations when its duty to preserve is triggered as any other party defendant. Safelite—a national auto glass repair and replacement company—sued its former store manager, Lockridge, alleging that he violated a non-competition and non-solicitation agreement by recruiting Safelite employees to his new employer, Caliber Collision via text message on his personal mobile iPhone. Shortly after Lockridge began work at Caliber, Safelite sent him a cease and desist letter outlining its concerns, which the Court found sufficient to trigger Lockridge's duty to preserve relevant evidence. Despite this warning and an eventual instruction from

counsel to preserve “documents, records, or communications,” six months later, Lockridge advised that his text messages were set to auto-delete every 30 days. By the time he discovered the phone’s auto-delete setting, the relevant text messages no longer existed.

The Court held that Lockridge had a duty to preserve his text messages starting at least as of the cease and desist letter, specifically rejecting his lack of sophistication as an individual party as a basis for leniency. Because the texts were irretrievably lost and were likely relevant (based on circumstantial evidence and phone records), the Court imposed sanctions under Federal Rule of Civil Procedure 37(e)(1). Although the evidence showed negligence rather than intent, the Court found prejudice, granted Safelite a permissive adverse inference instruction, and awarded fees and costs. Practically, this decision underscores the importance of (1) quickly recognizing when a duty to preserve may be triggered, (2) verifying and documenting the settings of any potentially relevant devices (particularly personal mobile phones), and (3) using third-party records or forensic techniques early to confirm whether critical ESI is at risk of being lost.

A key lesson here is the importance of device settings and early forensic analysis. By default, iPhones typically retain text messages indefinitely, so litigators should investigate when and how those settings may have been changed—particularly if a corporate “Bring Your Own Device” (BYOD) policy or the user’s personal preference alters the default setting. While counsel for Safelite sought the phone records from Lockridge to show the existence of text messages sent from Lockridge to the Safelite employees, counsel did not seek a forensic examination of Lockridge’s phone. Such an investigation could have revealed precisely when the text retention setting was modified (the preference file’s modification timestamp), which might have elevated the Court’s finding from negligence to intent. This highlights the crucial need for counsel (1) to give explicit instructions about preserving all forms of ESI early and ensuring preservation vs. relying on your client to understand how to take those steps, (2) to verify phone settings that might auto-delete relevant data, and (3) to consider a targeted forensic analysis when the timing and content of lost communications are central to the litigation.

In [Maziar v. City of Atlanta](#), the failure to preserve seemingly minor text messages—cost the City dearly by undermining its ability to secure summary judgment. In this retaliation case, the plaintiff, a former director of the Atlanta Mayor’s Office of Immigration Affairs, alleged that her termination was motivated by her complaints about discriminatory pay practices, mismanagement of COVID-19 relief funds, and failure to adhere to the City’s limited English proficiency policy. While the City contended that her firing was due to unprofessional behavior at a key meeting on April 29, 2021, a litigation hold was only issued four days after her termination on May 10, 2021. Unfortunately, no effort was made to search the supervisor’s personal or work phone for relevant messages, and when the supervisor left the City in December 2022, her phone was wiped—thereby erasing vital ESI.

The Court’s analysis, framed under Federal Rule of Civil Procedure 37(e), made clear that the lost text messages met all the prerequisites for sanctions: they should have been preserved in anticipation of litigation, they were irretrievably lost due to a failure to take reasonable steps, and they could not be replaced through additional discovery. Although the Magistrate Judge initially focused narrowly on “comparator evidence,” the District Court broadened the scope to consider the full range of potential evidence lost. While the Court acknowledged that a finding of bad faith (and thus sanctions under Rule 37(e)(2)) requires proof of an intent to deprive the opposing party of evidence, it ultimately determined that, despite the failure to preserve, there was no demonstrable bad faith on the City’s part. Nonetheless, the prejudice to the plaintiff—stemming from her inability to contextualize a cropped text message and recover additional communications—was sufficient to warrant sanctions.

As a remedial measure, rather than imposing an adverse inference instruction, the Court chose to deny the City’s summary judgment motion, thereby ensuring that the case would proceed to trial where the impact of the spoliated evidence could be fully assessed. In addition, the Court awarded monetary sanctions in the form of costs and fees for both the motions before the Court and for those incurred by the plaintiff in responding to the summary judgment motion.

The key lessons here are unmistakable: counsel must prioritize the prompt identification, preservation, and collection of all relevant ESI, especially from mobile devices, to avoid irreparable loss and subsequent sanctions. Failing to do so, even in seemingly straightforward employment disputes, can significantly tilt the scales of justice by depriving the opposing party of critical context and evidence necessary to substantiate its claims.

The [Jones v. Riot Hosp. Grp. LLC](#) decision underscores that deliberate deletion and coordinated spoliation of text messages can lead to severe sanctions—even case dismissal—regardless of the production of thousands of other messages. This takeaway is critical for practitioners, emphasizing that meticulous preservation of electronic communications is essential to avoid punitive measures under Rule 37(e)(2).

In this case, plaintiff Alyssa Jones, a waitress in Scottsdale, Arizona, brought claims against Riot Hospitality Group alleging Title VII violations and various torts. During discovery, defense counsel identified significant gaps in the text message records that Jones produced, noting that regular communication patterns had inexplicably ceased. A third-party imaging vendor later confirmed that messages exchanged with coworkers had been deleted, and depositions revealed that these coworkers had exchanged relevant messages about the case after the apparent cutoff.

The District Court found that Jones intentionally spoliated evidence by deleting text messages from her mobile phone and coordinating with witnesses to conceal communications from key time periods. Despite clear court orders and multiple deadline extensions to produce the missing messages, Jones and her counsel failed to comply, prompting the Court to order a neutral forensic expert to extract the evidence and ultimately assess nearly \$70,000 in fees and costs. On appeal, the 9th Circuit upheld the district court's ruling, rejecting Jones's arguments that her conduct was inadvertent or not prejudicial. The Court emphasized that the deliberate, selective deletion—supported by circumstantial evidence such as the timing and pattern of deletions—clearly demonstrated willful intent to obstruct discovery.

Ultimately, the case serves as a stark reminder that producing large volumes of other communications does not excuse the targeted deletion of relevant texts. Practitioners must ensure robust preservation protocols are in place and scrutinize data practices early in the litigation process. The decision highlights that courts are willing to impose the harshest sanctions when electronic evidence, once lost, cannot be restored—underscoring the vital importance of proactive, comprehensive data preservation strategies in ediscovery.

Preservation of Ephemeral Messaging

In [Two Canoes LLC v. Addian Inc.](#), failing to proactively identify and preserve ephemeral messaging data—in the form of WeChat messages—exposed a party to severe sanctions and left key evidence irretrievably lost. In this case, Two Canoes sought sanctions for spoliation after Addian’s CEO, Wolworth, failed to produce WeChat messages that were critical to the dispute over allegedly fraudulent N95 masks. The background is layered: Addian purchased masks from a Chinese supplier through Fisher and then resold them down a chain involving Aobvious and ultimately, Two Canoes. While Wolworth preserved emails and texts with Fisher, he did not preserve any WeChat communications. This becomes especially significant given WeChat’s design to delete messages automatically—after 72 hours for texts and 120 hours for multimedia—unless they are backed up, which Wolworth did not do, partly due to the loss of his cell phones.

The timeline in this matter is crucial. Addian’s duty to preserve was clearly triggered as of November 2020—before the 3M lawsuit—and continued through the subsequent litigation against Aobvious, where Addian was added as a third party. The Court focused on two key periods: messages between November 5, 2020, and October 2021 were lost, while those after October 2021 until February 2022 were not shown to be lost. Despite this, the Court found that Wolworth did not take reasonable steps to preserve the WeChat messages during the relevant period. With Fisher unresponsive to subpoenas, there was no alternative way to recover these messages, establishing the spoliation claim.

In its analysis under Rule 37(e)(2), the Magistrate Judge, Jose Almonte, recognized the complexity of determining prejudice and intent, noting that while it's challenging to assess the exact harm given that Wolworth primarily communicated by phone, the loss of the WeChat messages is undeniable. The Judge recommended deferring final decisions on both prejudice and intent to a jury—emphasizing that Wolworth's credibility will be central to whether his failure was intentional. This approach highlights the potential pitfalls of relying on mobile devices for preserving critical evidence without proper safeguards.

The key takeaway is clear: early, proactive planning and comprehensive custodian interviews are essential to identify all relevant data sources, including those on mobile devices and ephemeral messaging platforms. Counsel must ensure that clients have robust preservation protocols in place from the outset to avoid costly sanctions and the risk of adverse inferences at trial. Addressing these issues upfront is far more effective than attempting to mitigate the damage after data has already been lost.

Redacting Text Messages for Non-Responsiveness— Can You?

[We the Protesters, Inc. v. Sinyangwe](#) highlighted the importance of establishing clear, negotiated protocols for text message production in discovery to avoid disputes over redaction and relevance. In this case, the parties had agreed that all text messages in a chain—sent or received on the same day in which a search term hit—would be produced regardless of whether the initial message was deemed responsive or relevant. Under that agreement, plaintiffs produced thousands of text message strings with redactions for relevance, while defendants provided hundreds of unredacted strings. Defendants then objected to the plaintiffs' redactions, arguing that redacting for relevance was not permissible under their agreement, leading to a motion to compel.

Magistrate Judge Stein’s decision underscores a key point: without explicit, comprehensive agreements on how to handle the production of text messages—such as whether to redact non-responsive texts or produce entire chains—litigants risk court intervention to fill in the gaps. The decision references earlier cases like [Lubrizol Corp. v. IBM Corp.](#) and the leading Southern District of New York case, [Al Thani v. Hanke](#), to illustrate that unilaterally redacting information in text message chains, when no agreement on redaction exists, is not acceptable. The Court’s analysis reveals that the parties’ failure to address these nuances in their discovery protocol ultimately led to this dispute.

The takeaway is that effective ediscovery requires more than just an agreement to produce messages; it necessitates a detailed, written protocol that clearly defines what constitutes a document for production, how non-responsive material is to be handled, and whether redactions are allowed. Consistency across different sources of ESI is paramount, and parties are well advised to negotiate these details early on. This decision serves as a reminder that proactive and precise planning in managing text message discovery can save significant time, expense, and potential sanctions later in litigation.

The Need for an Exit Strategy and Mobile Devices

[Wegman v. U.S. Specialty Sports Ass’n, Inc.](#) made clear that failure to promptly return and preserve company mobile devices can severely prejudice an organization’s ability to safeguard critical evidence. In this case, DeDonatis—once the CEO of USSSA and subsequently placed on administrative leave—was ordered by the Court to return three mobile devices that the organization unequivocally owns, as evidenced by language in its employee handbook stating that all technology provided by USSSA is its property.

Prior to the hearing, DeDonatis had sought permission to create forensic copies of the devices before returning them, but the Court denied this motion. The Court emphasized that both parties were already aware of

the duty to preserve the information stored on those devices, and that DeDonatis' retention of these devices hindered USSSA's ability to collect critical evidence. Counsel for DeDonatis conceded ownership based on the employee handbook, which underscored the organization's preservation obligations. The devices were needed to determine what DeDonatis knew, when he learned it, what actions he took, and who else was involved, and his failure to return them frustrated the investigation and defense preparation.

The takeaways from Wegman are significant for practitioners dealing with mobile device discovery. With mobile devices now integral to business operations, organizations must proactively address issues of possession, custody, and control, as well as establish clear offboarding procedures that ensure the timely return and forensic preservation of devices. Delays can lead not only to the loss of critical data—through user deletions, automatic deletions, or physical damage—but also to costly and complicated recovery efforts, as highlighted by forensic experts. Ultimately, the decision underscores the necessity for organizations to have robust data preservation strategies in place to meet their evidentiary obligations and to mitigate the risks associated with the dynamic nature of mobile device data.

“Active, early preservation of text messages is now as necessary as email preservation was in the early days of ediscovery. Text messages remain the predominant form of communication on mobile devices and critical to telling a party’s story in litigation. The barriers that made mobile device collection difficult and expensive have given way to technology that allows any attorney or legal professional to remotely capture data defensibly the same day and immediately leverage it in litigation. What was difficult is now a few clicks away.”

– Matthew Rasmussen
Founder & CEO,
ModeOne Technologies

The Erosion of Protection of Legal Hold Notices

Several cases in the last few years have challenged the status quo that legal hold notices are presumptively privileged. Instead, a line of cases have emerged finding that legal hold notices can be subject to scrutiny—and ultimately compelled—when a preliminary showing of spoliation is made, underscoring the importance of clear preservation practices for ephemeral data.

Other decisions have begun to cut into the data that may be privileged, finding that where preservation is at issue, information about legal hold notices, may be relevant in certain situations. Counsel need to be aware of these lines of case law when they draft notices, planning for the potential discoverability of the data included in them.

Production of Notices Required Upon Showing of Spoliation

[In this antitrust litigation](#), the FTC alleges that Amazon employs anti-competitive strategies to maintain its monopoly power, and the FTC has moved to compel the production of document preservation notices and internal instructions regarding the use of ephemeral messaging apps such as Signal and Wickr. The FTC's request spans multiple time points—from as early as June 2019 through September 2023—reflecting a four-year investigation preceding the filing of the complaint in September 2023. Essentially, the FTC is asking Amazon to produce all litigation holds, preservation notices, or similar communications issued in connection with its duty to preserve evidence during this extensive investigation.

The Court's analysis was straightforward yet significant. Judge John Chun acknowledged that while litigation hold notices are generally shielded by attorney-client privilege or the attorney work-product doctrine, a preliminary showing of spoliation can overcome these protections. Citing relevant case law, the Court agreed that the requested documents might reveal whether Amazon failed to adequately preserve evidence during its investigation. However, instead of compelling production of the privileged

documents directly, the Court determined that the appropriate remedy was to order a 30(b)(6) deposition of an Amazon employee. During this deposition, the FTC will have the opportunity to inquire about key details—specifically, the timing and recipients of the litigation hold notices, the categories of information and data that were preserved, and the specific actions Amazon instructed its employees to take regarding preservation.

The key takeaway here is that a preliminary showing of spoliation can erode the privileged status of legal hold communications, allowing a compelling party to obtain critical preservation information via a 30(b)(6) deposition. This decision reinforces the need for organizations, especially those under long-term investigation, to engage in early and explicit discussions with custodians about their preservation obligations. As data increasingly flows through ephemeral messaging platforms, ensuring that proper legal hold notices are not only issued but also meticulously tracked becomes essential to avoid sanctions and adverse inferences down the line.

Other decisions on this issue to watch include [EEOC v. Formel D](#) (requiring production of legal hold notices following the spoliation of mobile device data); [Homeland Ins. v. Ind. Health Ass’n., Inc.](#) (“litigation hold notices are not per se protected by the attorney-client privilege” and “where a litigation hold notice merely ‘describes document retention practices or instructions for preservation, courts have rejected claims of attorney-client’ privilege”); [EEOC v. Aspire Reg’l Partners, Inc.](#) (preliminary showing of spoliation was sufficient to require production of hold notices).

When Key Information About Legal Hold Notices May Be Required

[Doe LS 340 v. Uber Techs., Inc.](#) came before the Court on a motion to enforce Pretrial Order No. 2 and compel Uber to produce information regarding its litigation hold and the scope of its preservation of electronically stored information (ESI). In this multi-district litigation, plaintiffs—alleged victims of sexual assault or harassment by Uber drivers—claim that Uber failed to implement adequate safety measures. The plaintiffs assert that Uber knew as early as 2014 that its drivers were engaging in sexual misconduct, and Pretrial Order No. 2, issued on November 3, 2023 by District Judge Breyer, was meant to secure the preservation of documents and ESI relevant to these allegations. Following the issuance of the order, the parties attempted to meet and confer on the scope of Uber’s preservation efforts and the terms of a protective order, but an agreement could not be reached. Consequently, the plaintiffs filed their motion on December 14, 2023, and although a final protective order was issued on December 28, 2023, Uber’s subsequent disclosures—delivered on January 4 and January 8, 2024—consisted only of a list of 15,700 current and past employees subject to legal holds, which provided merely job titles without any names, dates of issuance, or context regarding the underlying litigation.

Turning to the specifics, the Court’s attention was drawn to two critical areas of inquiry. First, the plaintiffs sought detailed information about the custodians under legal hold. They wanted the names, job titles, dates of employment, dates of issuance, and an explanation of which litigation or claim each hold pertained to. Second, the plaintiffs requested a full accounting of Uber’s sources of ESI—both custodial (data tied to individual employees, such as emails and Slack messages) and non-custodial (enterprise databases like Salesforce that are not tied to any one custodian). Additionally, the plaintiffs asked the Court to order Uber to suspend its company-wide document destruction policies, arguing that these policies might be resulting in the ongoing destruction of relevant evidence.

In its analysis, the Court reiterated that as soon as a party reasonably anticipates litigation, it has a duty to preserve evidence, which includes taking proactive steps such as suspending document retention policies and issuing legal holds. The Court rejected Uber’s argument that providing only job titles was sufficient under the Rule 26(f) checklist, emphasizing instead that basic details surrounding a legal hold—including the specifics of who was notified, when, and for what reason—are not shielded by attorney-client or work-product privilege. Citing recent precedent and the Sedona Principles, the Court concluded that the plaintiffs were entitled to a clearer picture of both the custodial and non-custodial sources of preserved ESI, and therefore granted the motion with respect to these disclosures.

The takeaway from this decision is straightforward: in complex litigation, particularly in a large-scale case involving hundreds or thousands of employees, parties must be prepared to provide detailed information about their preservation efforts. This includes a full accounting of legal hold notices and a comprehensive list of the electronic data sources being preserved. While the Court acknowledged that Uber’s disclosures regarding its document destruction policies were already sufficient, it made clear that the specifics of legal holds and ESI sources are critical to determining whether preservation obligations have been met. For practitioners representing large organizations, this ruling underscores the importance of tracking and disclosing detailed preservation efforts early on to ensure compliance with discovery obligations.

Additional Key Decisions from 2024

Multiple decisions in 2024 touched on key practice concepts for counsel to pay attention to in discovery strategy—again necessitating the need for early planning to identify issues and avoid unnecessary expense. While expense is always a factor, the key to effective ediscovery is often being able to see the forest for the trees and narrow in on what is key to telling your client’s story. The volumes of ESI make it easy to get lost in the noise, and technology advances to help resolve that challenge, counsel can focus on the key ESI that allows for strategic decision making.

“Effective and early communication within litigation teams is the key to both capitalizing on the opportunity with electronically stored information (ESI) to tell a story effectively and to navigate the intricacies of counsel’s obligations to produce sources of ESI like collaboration platforms, hyperlinked files, text messages and instant messaging. The right technology helps teams build innovative and cost-effective solutions. When paired with an early discovery strategy, it allows them to uncover key facts sooner and make more informed decisions for better case outcomes.”

– Joey Seeber
CEO, Level Legal

[Lubrizol Corp. v. IBM Corp.](#) illustrated that attempting to limit spoliation liability through a narrow interpretation of the duty to preserve—and through a FRE 502(d) order designed to shield intentional disclosures—can backfire by effectively waiving privilege over critical communications. Lubrizol alleged that IBM committed fraud and other torts in connection with an ERP software project and subsequently spoliated evidence by deleting electronically stored information from IBM personnel, including that of departed employees. Lubrizol contended that IBM’s duty to preserve evidence arose well before the complaint was filed in April 2021, pointing to a termination notice in April 2020, pre-litigation communications, hiring of outside counsel, and mediation that all indicated IBM’s awareness of potential litigation.

On the procedural front, IBM advanced two competing motions: one seeking a FRE 502(d) order to allow the production of documents without waiving privilege, and the other, by Lubrizol, to compel the production of communications concerning IBM’s document preservation efforts. The Court analyzed IBM’s FRE 502(d) request and, drawing on case law and the Sedona Conference’s principles, determined that such an order is limited to *inadvertent* disclosures rather than intentional ones. Moreover, the proposed scope was too broad—covering documents that could support IBM’s spoliation position while potentially allowing selective disclosure—and thus the Court denied IBM’s motion.

Turning to Lubrizol’s motion to compel, the Court required IBM to produce a detailed log and non-privileged documents about its preservation efforts, including legal hold notices and internal communications regarding the deletion of emails from former employees. Crucially, by asserting that its duty to preserve did not arise until after the complaint filing, IBM effectively waived its privilege over communications that would have otherwise established that its duty to preserve began much earlier. The Court applied a three-factor test under Ohio law (from [Hearn v. Rhay](#)) and found that IBM’s delay in identifying custodians and preserving evidence undermined its position.

The key takeaways from this decision are twofold: first, Federal Rule of Evidence 502(d) does not extend to intentional disclosures, and second, the timeline for a preservation duty is critical. IBM's attempt to define its preservation obligation narrowly—claiming it did not begin until post-complaint—resulted in a waiver of privilege over pivotal communications that were vital to Lubrizol's spoliation claim. This ruling serves as a reminder to companies and their counsel to clearly establish and act upon their preservation obligations well in advance of litigation to avoid severe sanctions and the loss of critical evidence.

[Bocock v. Innovate Corp.](#) is a real-world wake-up call in responding to written discovery: if you wait too long to provide specific discovery responses and rely on generic, boilerplate objections, you're risking a waiver of your objections and a hefty cost sanction. In this case, 26 plaintiffs filed a complaint on June 23, 2021, and while most of their claims got dismissed by October 28, 2022, the defendants didn't sit around. Almost two years after the complaint was filed, on May 5, 2023, the defendants served interrogatories and requests for production. The plaintiffs got a 15-day extension, pushing their deadline to June 20, 2023—but what they delivered was a single, collective seven-page response filled with general objections that were nothing more than boilerplate, duplicative, and untethered to any specific interrogatory or production request.

The Court wasn't having it. It looked at the timeline—the sheer delay between the complaint filing and the plaintiffs' motion—and noted that for over 168 days, the plaintiffs had failed to provide any substantive discovery responses for all 26 plaintiffs. When pressed, the plaintiffs didn't try to justify their failure to provide specific responses; instead, they argued that because there was no case scheduling order in place and because of the sheer number of plaintiffs, cost shifting wasn't warranted. The Court dismissed that argument as frivolous, holding that the rules are what they are: under Delaware's Chancery Court rules (which mirror the Federal Rules), objections need to be specific. The Court pointed to the requirements of Rules 33 and 34, which demand that each interrogatory and request be answered separately and fully unless properly objected to with specific

grounds. As a result, the Court granted the motion to compel and ordered the plaintiffs to serve proper discovery responses within five days, and it also ordered cost shifting because the plaintiffs' conduct wasn't justified.

The takeaways here are as clear as day: if you're handling discovery for a multi-plaintiff case, you better get your act together from the get-go. Waiting too long to nail down specific objections is a recipe for disaster—it not only waives your right to object but also invites severe sanctions under Rule 26(g) and the case law. This decision is a brutal reminder that general objections just won't cut it anymore following the 2015 amendments. You need to dig into the details early on, craft tailored, specific responses, and get them in on time. Otherwise, you're setting yourself—and your client—up for a major headache down the road.

Preservation of Video

[Nagy v. Outback Steakhouse](#) involves a motion for spoliation and sanctions brought by the plaintiff against Outback for failing to adequately preserve surveillance video of her slip and fall in one of its restaurants. The plaintiff, who was dining with friends and experienced a serious fall resulting in a fractured hip and femur, contends that crucial video evidence—which could show whether a greasy substance contributed to her fall—was not properly preserved. Although Outback did preserve a short 19-second clip and later a 27-minute segment (capturing a narrow window around the incident), much of the video that could have shed light on conditions before her fall was overwritten, as the camera system operates on a seven-day loop.

The incident took place in the area just outside the restaurant's kitchen, where the plaintiff claims a slippery substance was present. Outback's manager testified that routine checks were supposed to catch and clean any spills; however, no formal incident report was created at the time. Instead, after the accident, the manager reported the incident to the insurance claims administrator, and a preservation letter was eventually sent 12 days later, demanding that all surveillance footage be kept for a full

day before and after the event. Despite this, Outback's internal practices fell short—without a clear policy instructing managers on the exact duration of video to preserve, the manager only saved minimal footage before the automated overwriting process took effect.

In its analysis, the Court focused squarely on the duty to preserve evidence under Rule 37(e). It held that because litigation was clearly foreseeable—given the severity of the plaintiff's injuries and the immediate reporting to the claims administrator—Outback had an obligation to preserve a complete record of the incident, including footage from a reasonable period before the fall. The Court underscored that the selective preservation, which resulted in only a brief snapshot of the period before the plaintiff fell, was not acceptable. The evidence was not recoverable by other means, and the fact that Outback's manager was left without specific guidance contributed to an inference of intent to deprive the plaintiff of crucial evidence. Consequently, the Court permitted an adverse inference instruction to the jury, indicating that the lost footage might be presumed to be unfavorable to Outback.

The takeaways here are significant for any establishment that relies on surveillance as part of its risk management strategy. First, organizations must implement clear, specific policies for preserving video evidence when an incident occurs—simply relying on a manager's discretion is not enough. Second, in cases where critical video evidence is selectively preserved or lost, courts are prepared to draw adverse inferences against the party responsible. This decision reminds practitioners that a robust, well-documented preservation policy is essential to avoid sanctions and ensure that key evidence is available for litigation.

General Objections

[Byte Fed., Inc. v. Lux Vending LLC](#) underscores the necessity for tailored, specific discovery responses in trademark litigation, rather than relying on generic, boilerplate objections that can lead to delays and increased costs. In this trademark infringement dispute, the plaintiff initially served a subpoena on Cardamone Consulting Group, LLC (“Cardamone”) on May 26, 2023, requesting production of materials by June 8. Cardamone retained counsel on June 5—just three days before the deadline—and requested an extension, which the plaintiff granted until June 16. Rather than responding substantively, Cardamone filed a motion to quash on June 12, arguing that the subpoena sought confidential information and was unduly burdensome.

Later, after Cardamone was added as a party in August 2023, the plaintiff served a first set of requests for production on September 21, 2023. When Cardamone finally served its responses and objections on October 23, 2023, they failed to produce any documents or specify a date for production. The Court denied Cardamone’s motion to quash the subpoena on October 26, 2023, and compelled it to respond. On November 7, 2023, the plaintiff escalated matters by filing a motion to compel the production of documents responsive to the first set of requests, as well as seeking attorney’s fees for the motion. Cardamone produced some documents on November 9, 2023, but maintained objections to nine requests for production.

The Court’s analysis turned on the relevance, non-privilege, and proportionality of the discovery requests under Rule 26. For instance, Request No. 7 sought electronic records from three corporate email accounts based on a Boolean search query provided by the plaintiff. Cardamone objected, calling the request vague and incomprehensible, but the Court overruled the objection due to insufficient explanation from Cardamone on what was unclear. Similar boilerplate objections were dismissed for requests related to website traffic data, financial records, and digital advertising materials. Additionally, the Court rejected arguments that the client’s unfamiliarity with ediscovery practices should excuse such shortcomings, emphasizing that it is the responsibility of counsel to assist their client in meeting these obligations.

Ultimately, the takeaway is straightforward: ineffective, generic objections and delayed, non-specific discovery responses can result in the Court overruling those objections and awarding costs against the party that fails to comply. This case reinforces the importance of understanding the evolving ediscovery landscape, where precise, individualized responses are essential for efficient litigation management and cost control.

The Importance of Following Retention Policies

[Lopez v. Apple Inc.](#) highlighted how a post-complaint change in data retention policy can lead to crippling sanctions when crucial evidence is not preserved. Here, plaintiffs alleged that Apple recorded private conversations through a false activation of Siri—recordings that were later disclosed without consent—and then failed to preserve the majority of this sensitive data. Originally, Apple’s retention policy kept Siri recordings for six months with an associated Assistant ID, extended them for an additional 18 months after disassociation, and maintained a small subset for five years for quality review. However, following a July 2019 Guardian article exposing these practices, Apple revised its policy in August 2019 and implemented a new opt-in program in October 2019—two months after the complaint was filed—thus triggering its duty to preserve evidence under litigation.

Magistrate Judge Sallie Kim’s decision, dated June 17, 2024, centers on the fact that once litigation was foreseeable, Apple was obligated to suspend its auto-deletion processes and retain all relevant data. Despite this, Apple allowed its standard deletion schedule to continue, resulting in the loss of millions of Siri data points that could have substantiated the plaintiffs’ privacy and misuse claims. The Court criticized Apple for not seeking a court order to clarify its preservation obligations, emphasizing that the burden to preserve lies with the party that anticipates litigation. Although the question of whether Apple intentionally deleted the data was left to a jury, the Court imposed severe sanctions under Rule 37(e)(1), effectively barring Apple from later arguing that the absence of the data undermined its defense.

The decision reinforces that proactive and robust preservation practices are critical when sensitive electronic data is at stake. The Court's sanctions prevent Apple from using the missing data as a shield against claims such as lack of standing or to contest the extent of class-wide damages. For attorneys, this ruling underscores the importance of establishing clear retention protocols and engaging with the Court early to determine the scope of a preservation obligation—rather than relying on automated deletion schedules that can inadvertently destroy vital evidence.

Ultimately, *Lopez v. Apple Inc.* serves as a stark reminder to all organizations that, when litigation looms, any changes to data retention policies must be carefully managed. Failing to do so not only risks significant sanctions but also can irreparably harm a company's ability to defend itself in privacy and data misuse cases. Counsel must ensure that their clients' data preservation practices are up to date and aligned with their litigation exposure to avoid similar pitfalls.

Privilege Considerations

A second decision in the [FTC v. Amazon](#) matter highlighted the importance of managing privileged documents across multiple investigations, as failure to properly assert privilege and promptly rectify mistakes can lead to waiver, even in complex cases.

In this decision from August 1, 2024—issued by United States District Judge John Chun—the FTC moved to compel the production of 17 documents that Amazon had previously produced *in connection with multiple FTC investigations* and then subsequently clawed back during the litigation, asserting privilege.

The FTC argued that by redacting documents intentionally and failing to promptly clawback inadvertently produced materials, Amazon effectively waived its privilege across several categories of documents, which include internal memos, presentations, and chat messages.

The Court’s analysis hinged on the application of Federal Rules of Evidence 502(b) and 502(d). The FTC contended that the 502(d) order should not protect documents produced during pre-suit investigations, and the Court agreed—clarifying that such an order applies only to documents produced during the current litigation. Furthermore, the Court found that Amazon’s decision to produce redacted versions of documents, such as the May 4th memo, was a deliberate act rather than an inadvertent disclosure. Additionally, the delays in clawing back certain documents—18, 49, and 21 days respectively—were deemed unreasonable under Rule 502(b), meaning that Amazon failed to meet the standard required to preserve privilege.

Ultimately, while the Court deferred the final determination of privilege regarding the chat messages in IC-9 and the July 14th presentation through in-camera review, it ruled that for the majority of the documents, Amazon had waived its privilege. The takeaway is clear and challenging: when managing discovery across multiple investigations and subsequent litigation, parties must implement robust, coordinated processes to ensure that privilege is consistently asserted and that any errors in production are rectified promptly. This decision serves as a critical reminder that even slight delays or strategic decisions in document redaction and clawback can have far-reaching consequences in complex litigation.

“Managing multiple databases across investigations and subsequent litigation is complex, and it requires effective communication between the disparate legal teams to ensure that the decisions made on privilege issues are consistent and in line with the Federal Rules of Civil Procedure. It is incumbent on counsel to advise of these critical issues to allow those handling the ESI to track and take appropriate action to protect client’s data.”

– Joy Murao
Founder and CEO,
Practice Aligned Resources

Manner of Production

The Court in [Partners Insight, LLC v. Gill](#) highlighted the importance of requesting clear and specific terms for the format and manner of producing ESI to avoid disputes and ensure efficient handling of data. Here, the plaintiffs sought to compel the production of documents in native format with metadata following an initial production in TIFF format by defendants, which did not include any specification of how the documents should be organized or provided.

The plaintiffs contested that the produced files lacked proper organization and clarity about which discovery requests the documents were responsive to. The Court's analysis focused on Rule 34(b)(2)(E) of the Federal Rules of Civil Procedure, which governs the form and manner of document production. The Court found that defendants had met the requirements by providing TIFF images with metadata, as they were reasonably usable and retained the necessary information from the original emails.

The Court emphasized that the plaintiffs had not *explicitly specified* in their requests for production that they required native format documents, which would have compelled the defendants to comply with that request. This highlights the common interpretation and language of Rule 34 that says, unless explicitly stated, a producing party may deliver documents in any reasonable format.

The Court also assessed the organization of the production, what we refer to as manner of production, and found that defendants' method of producing documents as they were maintained in the ordinary course of business, while not perfectly aligned with the plaintiffs' desires for organization, complied with the general standards set forth by Rule 34. Ultimately, the Court denied the plaintiffs' motion to compel and emphasized that the purpose of ESI production is to ensure accessibility and usability, which the defendants had achieved.

The key takeaway here is that when requesting ESI, parties should be very specific about the format (native vs. TIFF, etc.) and manner of production (organization and metadata fields). Courts are not knowledgeable about the value of having native data vs. TIFF images—it is incumbent on counsel to both request and be prepared to advocate for that format of ESI. Failure to do so can result in disputes that could otherwise be avoided. Moreover, the case reinforces the importance of providing clear instructions and establishing ESI protocols upfront, as courts generally will not require a producing party to reproduce information in a specific format unless it was clearly requested or there is a compelling reason to do so.

Effective ediscovery hinges on precise and detailed discovery requests. Litigators must explicitly state the desired form and organization of documents to avoid default productions that may not meet their review needs. Failing to do so, as demonstrated in *Partners Insight*, means that even if the documents are produced in a less-than-ideal format, they will likely be deemed acceptable if they reflect the way information is normally maintained. This decision reinforces the importance of negotiating tailored ESI protocols at the outset of litigation to ensure that the production format, metadata, and overall organization align with the requesting party's requirements.

How the Inadvertent Production of Documents Can Lead to Sanctions

[Cahill v. Nike, Inc.](#) puts the spotlight on an issue exacerbated by the ease of sharing ESI—that even inadvertent disclosures of confidential documents subject to a protective order can trigger sanctions if not promptly remedied and properly communicated.

In this proposed class action, plaintiffs alleged that Nike systematically discriminated against women regarding salary and promotions. While the plaintiffs' class certification motion was pending, Nike moved to seal parts of its filings containing sensitive employee information. Simultaneously,

several non-media party organizations—including the Oregonian—sought to intervene to gain access to the sealed documents. The Court partially granted both motions, allowing limited access for challenging the stipulated redactions while denying further unsealing until after the class certification motion was resolved.

After the class certification motion was denied in September 2022, the Court granted media organizations' motion to unredact some documents, but Nike subsequently appealed, resulting in a stay of the order by the Ninth Circuit. Fast forward to January 2024, when one of the plaintiffs' counsel met with a reporter from the Oregonian. During that meeting, the reporter disclosed that he had obtained a declaration containing serious allegations of sexual harassment and assault against a Nike employee, prompting counsel to compile and email a packet of internal survey responses on workplace culture.

Unbeknownst to counsel, the packet included documents that were protected by the existing protective order. Although the reporter initially agreed not to run the story, he later refused to return the inadvertently disclosed documents. Plaintiffs' counsel sought the Court's assistance to recover those documents on January 25, 2024. Nike learned of the disclosure only through the subsequent motion and then moved for harsh sanctions against counsel under Rule 37(b), seeking everything from monetary penalties and cost awards to disqualification of counsel and even a venue change.

In its analysis, the Court made it clear that the inadvertent disclosure of unredacted survey responses—which revealed confidential internal information, including the names of female executives—constituted a violation of the protective order, regardless of the lack of bad faith. While acknowledging that heavy-handed litigation tactics are common in high-profile cases, the Court ultimately found that there was insufficient evidence to support claims of deliberate misconduct. Consequently, the Court imposed only cost sanctions related to the motion and declined to impose additional monetary penalties, evidence exclusion, venue transfer, or counsel disqualification.

The key takeaway is that counsel must exercise utmost caution when handling documents covered by a protective order. Even accidental disclosures can have serious consequences if not immediately reported and remedied. This decision reinforces the necessity for rigorous document review procedures and timely communication with all affected parties, as well as for developing robust internal protocols to prevent such errors in high-stakes litigation.

Lessons in Drafting an FRE 502(d) Order

[In re TikTok Inc. In App Browser Privacy Litig.](#) demonstrated that a carefully crafted FRE 502(d) order is vital for safeguarding privileged communications during ediscovery, especially when inadvertent disclosures occur. In this case, plaintiffs allege that TikTok unlawfully intercepts users' communications on third-party websites via its in-app browser by inserting JavaScript that tracks keystrokes and captures entered data. The claims span violations of the Federal Wiretap Act, state anti-wiretapping statutes, data privacy, consumer protection laws, and common law privacy claims, making this a high-stakes matter in the realm of digital privacy litigation.

What sets this decision apart is that, rather than a contentious motion practice, the parties jointly stipulated to an order addressing inadvertent production. This order is not merely a procedural formality—it is a strategic tool designed to prevent any waiver of attorney-client privilege or work-product protection due to the inadvertent production of electronically stored information (ESI) within the litigation pending before the Court. The order explicitly states that any such disclosure will not constitute a waiver and clearly delineates its scope, covering everything from deposition transcripts and discovery responses to affidavits and trial testimony.

The Court's analysis emphasizes that the FRE 502(d) order functions as an "insurance policy" against the inadvertent disclosure of privileged information. It explains that while the three-step analysis required under Rule 502(b) can be burdensome, a properly implemented 502(d) order

removes that burden by ensuring that any production of privileged material in this litigation will not be deemed a waiver. Moreover, the order provides a detailed process for clawing back inadvertently produced documents—setting deadlines and procedures to address any errors—which is especially critical in complex matters where multiple data sources and high volumes of information are involved.

The key takeaway is clear: litigators must incorporate a tailored FRE 502(d) order early in the discovery process to protect sensitive materials from inadvertent disclosure and potential sanctions. This decision offers a robust template that can be modified to fit the specific needs of any case. However, it is crucial that counsel customize the language to address the nuances of their particular data sources and case context, rather than simply copying a model order. Proactive planning and meticulous coordination can mitigate the risk of costly sanctions and preserve the integrity of privileged communications throughout litigation.

Conclusion

While the debate of discovery vs. ediscovery may rage on, what you call this complex area of law matters little when compared to whether you understand your obligations in this ever changing area of the law. The targets are constantly moving—technological advancements in how users create, store, send and receive data keep happening and the issues inherent in them with regard to how that ESI is preserved, collected, and produced are complex. But the opportunity for leveraging ESI litigation—particularly in civil cases that are won and lost on the documents—is exponential.

Witnesses write everything down today. There's no more guessing what he said or what she knew—it all exists in the ESI. The key is wading through the noise, figuring out how to meet your obligations effectively and then *really leveraging* discovery strategy to achieve the best outcome for your client. In litigation, winning can take any number of forms—settlement, limited, focused, cost-effective discovery, summary judgment, or outright victory at trial to name a few. But what has always been clear to litigators is this—finding and focusing on the key evidence for a matter is the key to winning. And ESI lets you do that better and faster.

Our hope is that this year's report gives you insights into how to effectively create that discovery strategy that allows you to win for your clients—whatever form that takes.

Acknowledgements

We would like to express our deepest appreciation to our Partners for their invaluable support in helping us bring the 2024 Case Law Year Report to fruition, providing a comprehensive analysis of the latest issues in ediscovery and helping legal professionals stay ahead of the curve through their service and technology offerings.



Authored and edited by industry expert Doug Austin, [eDiscovery Today](#) is the only daily go-to resource for eDiscovery and eDisclosure professionals seeking to keep up with trends, best practices and case law in electronic discovery, information governance, cybersecurity, data privacy and artificial intelligence.



Level Legal makes legal human. The Dallas-based forensics, eDiscovery, managed review, and consulting company delights law firms and corporations through industry-best customer service that excels in dependability. This concierge approach to outsourced legal services delivers peace of mind. For more information, visit [levellegal.com](#).



ModeOne's patented SaaS framework offers the first truly remote and targeted solution for same-day collection of targeted data from Apple iOS and Android mobile devices for evidentiary, compliance, and investigation purposes. Anywhere in the world. Without the need for a physical collection kit or onsite forensics personnel. To request a demo or talk to us about your needs for collecting mobile device data click here; <https://modeone.io/#contact>



[Practice Aligned Resources](#) (PAR) is a legal technology consulting and education company dedicated to delivering tailored solutions to its clients and community. Our diverse clientele includes corporate legal departments, government agencies, and law firms of all sizes nationwide. We specialize in various practice areas, ranging from litigation support, including eDiscovery and trial assistance, to information governance, such as data mapping and legal holds, as well as public records response, including video and body camera redactions.

eDiscovery Assistant

Your Strategic Command Center for Discovery

Litigators need more than information—they need clarity, agility, and foresight to take control of discovery with confidence. Our platform centralizes the essential tools legal teams rely on, combining expert-curated case law, rules, strategic resources, and on-demand discovery education in a structured system that empowers decisive action.

Navigate Discovery with Confidence

- ✓ **Command Every Issue** – Our proprietary issue-tagging system and interactive dashboard provide instant insight into evolving discovery challenges.
- ✓ **Stay Ahead** – Gain access to continuously updated case law and rules, curated to align with the realities of modern litigation.
- ✓ **Make Informed Decisions Faster** – AI-generated case summaries, actionable checklists, and practical forms streamline strategy and execution.
- ✓ **Adapt in Real-Time** – Whether shaping legal holds, crafting ESI protocols, or preparing for motions practice, our structured system ensures nothing is missed.
- ✓ **Elevate Your Expertise** – Our discovery education hub delivers concise, expert-led training to sharpen your approach.

We don't just provide information—we illuminate the path forward, ensuring you stay ahead of evolving discovery challenges and lead with confidence.

Ready to take command of discovery? [Contact us for a demo](#) today or sign up for a [free 7-day trial](#) today!

Contact

eDiscovery Assistant LLC
2945 Juilliard Street
Boulder, Colorado 80305

 www.ediscoveryassistant.com

 info@discoveryassistant.com

 [/company/ediscovery-assistant™/](https://www.linkedin.com/company/ediscovery-assistant/)