

eDiscovery Case Law Year in Review

2023



TABLE OF CONTENTS

01 Introduction

09 Issues in eDiscovery

12 Report Structure

13 Part I: Takeaways from 2023

39 Part II: Key Areas to Watch

42 Conclusion

43 Acknowledgments

2023 CASE LAW REPORT

Introduction

Welcome!

Each year as we sit down to write this report, we look back at the events that shaped 2023, how they impacted litigation, and the role of electronically stored information (ESI) in those matters. Although the events of a year are often not reflected in the courts for several years, it is instructive from a risk management perspective to think about what will be at issue and how both organizations and counsel need to be prepared for the challenges coming their way and how to plan for them.

2023 was a year full of high-stakes legal battles, with the spotlight repeatedly falling on the critical role of the discovery of ESI. From disputes over images, video, and ephemeral messaging to the repercussions of failing to preserve ESI or comply with discovery obligations, the consequences have been significant:

- The DOJ faced [numerous challenges](#) in collecting and preserving crucial digital image and video evidence in preparation for hearings and trials following the January 6th Insurrection at the Capitol.
- In August 2023, the United States District Court for the District of Columbia [entered default judgment against Rudy Giuliani](#) for his failure to preserve data from multiple mobile devices and willful neglect in failing to meet multiple court-ordered discovery obligations.
- The crypto-industry and ephemeral messaging became the focal point of the month-long [criminal trial of Sam Bankman-Fried](#), the former CEO of the now defunct FTX, who deliberately deleted incriminating online posts, messages, and other pertinent data from platforms such as Twitter (now “X”), Slack and Signal. Witnesses also testified that Mr. Bankman-Fried [ordered the use of Slack and Signal to communicate](#), required employees to make messages ephemeral so they could not be kept, and to set automatic deletion at 30 days.

While those high profile matters represent less than 1% of the litigation we face daily, they are examples of the issues present in almost every single matter, large or small. The basic tenet of civil litigation — that cases are won and lost on the documents — has been turned on its head by ediscovery. With the change to Rule 34 in 2006 adopting ESI, every message, post, tweet, image, video, email, link to a document, comment, or chat — from a myriad of sources of ESI — is potentially discoverable and governed by the same rules as a “document.” Finding, keeping and presenting that information effectively to a factfinder poses challenges in both small and large stakes matters. The key is to know what sources of ESI are implicated in your matters and how to handle them.

This year’s report dives into how courts are addressing a variety of the sources of ESI that have become mainstream for users to create, store, send and receive data together with counsel’s obligations to preserve, collect and produce that data under the Federal Rules of Civil Procedure and their state equivalents.

Integrating Generative AI in eDiscovery Case Law

The public unveiling of ChatGPT in March 2023 by Open AI and the potential use cases of generative AI (GAI) in the legal profession drove the narrative for much of the year. That will carry on for years to come as the technology improves and there are more and more uses for it. To date, the best use for integrating GAI is its ability to summarize text. As such, [eDiscovery Assistant leveraged GPT 3.0](#) initially to create summaries of the then 34,000 decisions in our eDiscovery Assistant case law database (we are now at over 35,000). But even that summarization functionality has its limitations – we found that summaries of appellate decisions with dissenting or concurring opinions looked to the final lines of discussion when drafting the ruling of the court. That meant that the dissenting opinion — always the final text to an appellate case — caused the summary to reflect the dissenting opinion instead of the majority, requiring manual removal of that text to re-run an accurate summary. That’s just one example of the detail of issues that need to be considered in leveraging GAI.

We also found in using GAI for summarization that the newer ChatGPT Turbo 3.5 and 4.0 are infinitely smarter than their predecessor 3.0. The newer models do a better job of understanding the intricacies of ESI and ediscovery issues, and tend to vary sentence structure as well, making the summaries more readable.

We get a number of questions from our users and prospective buyers asking about whether GAI case law is included in eDiscovery Assistant. The answer is that as soon as there are any discovery decisions on GAI, they will be added with a corresponding issue tag to make finding them just a click away. As of this report writing, the only reported case law on GAI stems from lawyers attempting to use ChatGPT as a legal research tool, which, as we have seen [repeatedly](#), may result in both monetary sanctions as well as having serious implications for an [attorney's license to practice law](#).









The Heightened Role of Case Law in eDiscovery



As lawyers and legal professionals, the default position on case law is to leverage it when you need to make an argument. That works effectively when there are one or two or even several new decisions each year in a substantive area of the law, but not in ediscovery where we have seen an average of 5000 decisions a year in the last few years. The volume of ediscovery case law since the early 2000's has increased so exponentially that lawyers and legal professionals now need to be on top of what is happening in case law to allow them to properly assess both their own and client obligations as to new and novel sources of ESI. The wait and see approach is no longer viable.

Case law plays a crucial role in educating litigators and other legal professionals on issues related to ediscovery. 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 decisions from 2023 highlight, perhaps more than ever, the need for clients and their counsel to be aware of the ever evolving list of sources of ESI that are discoverable and the complexity of identifying, preserving, collecting and providing that information in discovery. Counsel now need to be prepared to deal with these data sources out of the gate for a matter, and the timelines imposed by the courts and the [Federal Rules of Civil Procedure](#) do not provide wiggle room for getting up to speed. Complex issues abound for counsel including, for example:

-  Handling documents that appear only as a link in an email and not as a physical attachment
-  Whether a collection tool captures the unicode of an emoji correctly and the review tool displays the same emoji originally sent by the custodian
-  How to review and produce instant messaging and Teams data effectively
-  How much context to provide around responsive messages captured by search terms in collaboration, text or instant messaging platforms like Slack, Teams, Signal, iMessage, etc.
-  How to request information regarding the algorithm of facial recognition technology to demonstrate or disprove inherent bias
-  What ephemeral data is, what applications allow for ephemeral settings, and how to handle preservation of that data when the duty to preserve arises
-  How to set up review effectively to minimize the cost of creating and producing a privilege log
-  Understanding the scope of proportionality, how to apply it and how to make an effective argument with specific factual showings

-  Leveraging tools to let counsel get in the data and use that early knowledge for strategic decision making
-  Advising clients on allowing the use of personal devices by employees for work

This list barely scratches the surface of the complexity we face in ediscovery. Counsel's obligations under [Federal Rule of Civil Procedure 26\(g\)](#) and its state equivalents are more extensive than ever and require that counsel certify, "after a reasonable inquiry" that all disclosures are complete and correct as of the time they are made, that any discovery request, response or objection is consistent with the FRCP, not intended to harass, cause unnecessary delay or "needlessly increase the cost of litigation", and that the request is neither unreasonable or unduly burdensome.

These obligations mean not only that counsel cannot put their heads in the sand, but, as we will see in a discussion of decisions below, that doing so may have dispositive results for their clients' matters. This year's decisions demonstrate that more and more judges on both the federal and state levels are becoming increasingly savvy about issues in ESI, and their corresponding expectations of counsel to present specific facts supporting their arguments on ediscovery issues.

Distribution of Case Law in 2023

While the volume of civil cases filed in the United States District Courts declined by 8%¹, 2023 saw a 10% increase in the number of ediscovery decisions at 5216. 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.

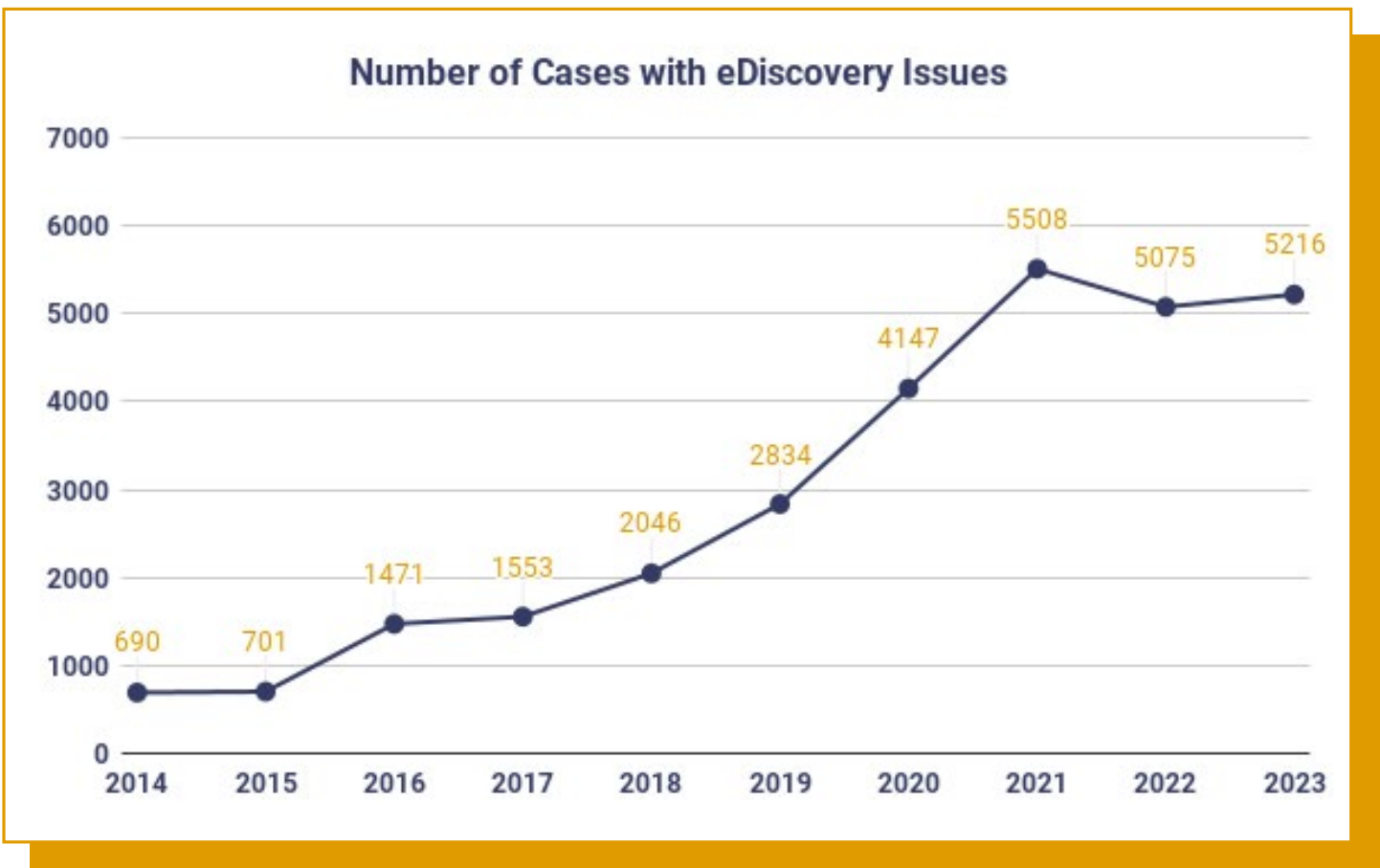
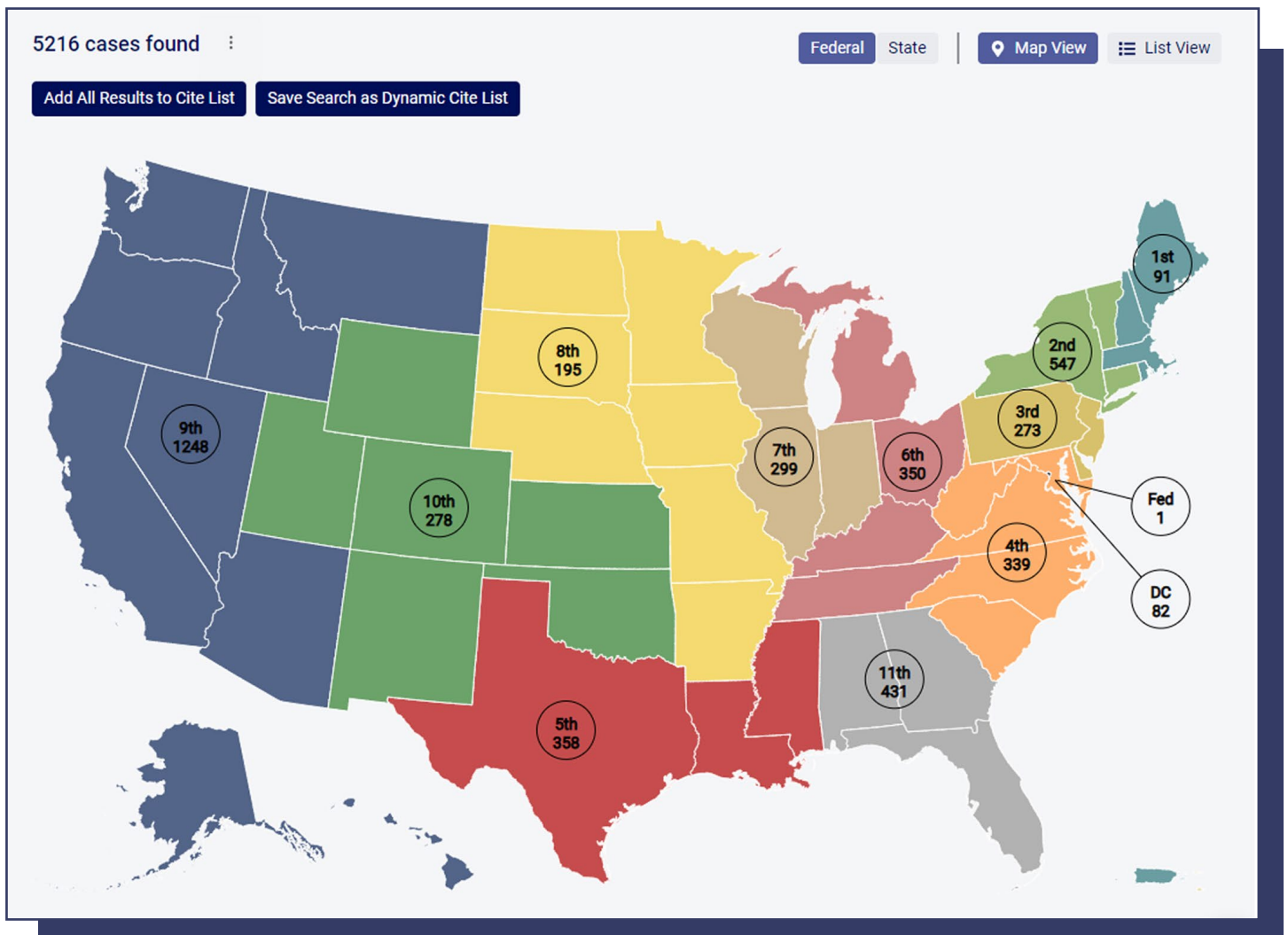


Chart 1 – Number of eDiscovery Decisions since 2014

¹ <https://www.uscourts.gov/statistics-reports/federal-judicial-caseload-statistics-2023>; the number of decisions listed includes all decisions added to our database as of the date of this report.

Maps 1 and 2 from eDiscovery Assistant show the breakdown of decisions across the federal and state courts in 2023. 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 2023

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 80 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 using boolean parameters to narrow a search, such as using Dismissal with Sanctions to narrow results to decisions including both issues. Chart 2 below shows the top twenty issue tags in the eDiscovery Assistant platform for 2023. The individual issue analysis sections of this report use boolean queries of the database to highlight issues.

As the chart reflects, and for the third straight year, failure to produce, proportionality and sanctions are the top issues. Those issues represent high level inquiries, and when coupled with other issues in a search string in the database allow users to drill into specific queries (e.g. Failure to Produce and Slack). Climbing up the list of issues this year is Redaction, with an uptick from 276 decisions in 2022 to 324 in 2023, and Cost Recovery, which grew exponentially from 173 decisions in 2022 to be one of the top ranking issues in 2023 at 945 cases. A complete listing of the breakdown of all 83 issue tags is available [here](#).

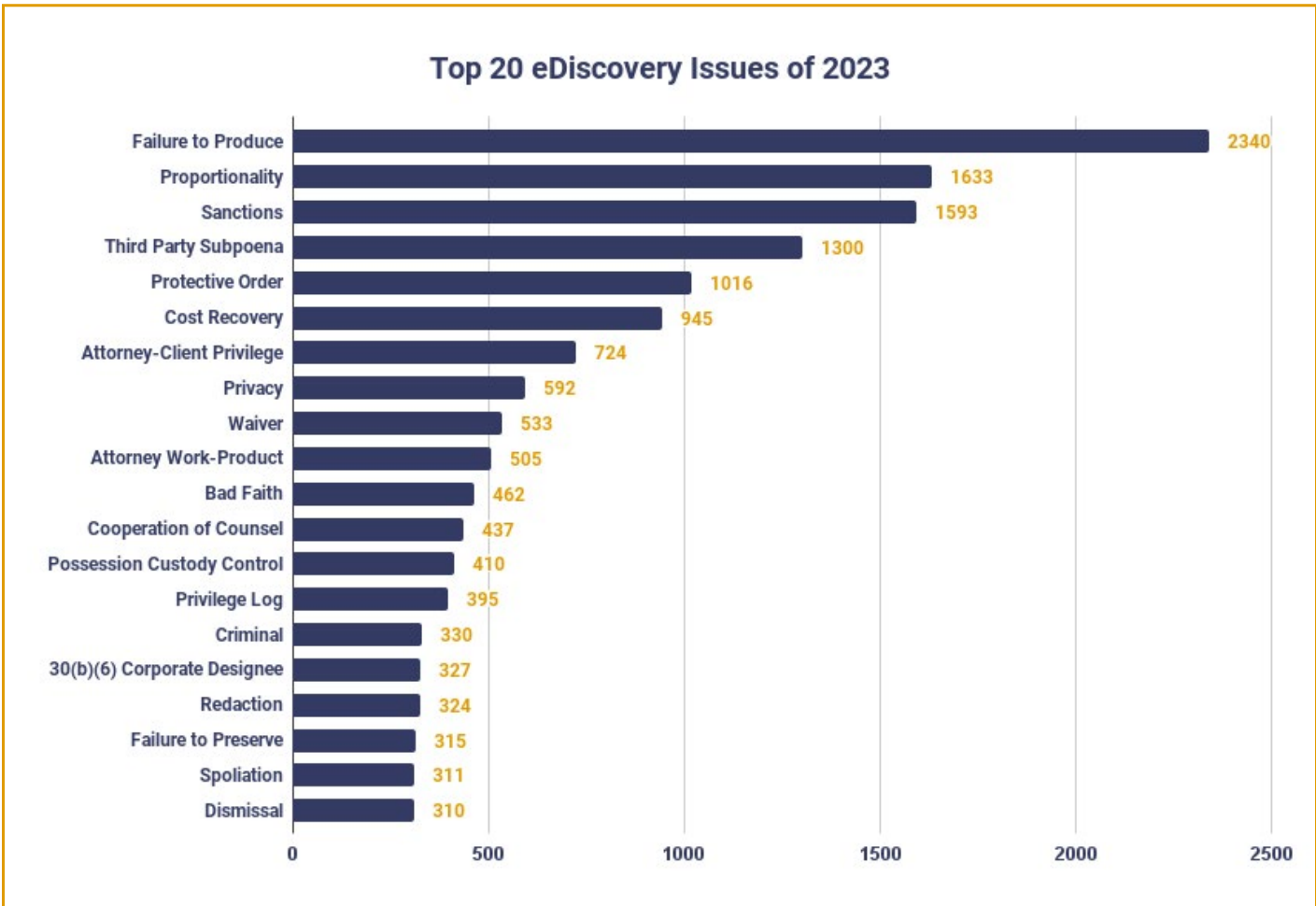







Chart 2 - Top 20 eDiscovery Issues of 2023

2023 also saw the addition of multiple new Issue Tags in eDiscovery Assistant following the development of specific areas and focus in the case law decision database. Those Issue Tags are:

-  **SIGNAL** – A mobile device application for instant messaging, voice and video calls with end to end encryption. Users of the app can send instant messages, voice notes, photos, videos and other files to an individual or a group. This issue is added when data from Signal is requested or analyzed in discovery.
-  **EMAIL THREADING** – Email threading refers to the process of organizing and grouping related email messages within a collection of electronically stored information (ESI) to facilitate the review and analysis of these emails during legal investigations or litigation. There are multiple technical and legal issues with email threading, and this issue tag is applied to content in the application that discusses or analyzes those issues including how they are produced and included on a privilege log.
-  **FACIAL RECOGNITION TECHNOLOGY** – Facial recognition technology works by identifying and measuring facial features in an image or video. This tag is added to content analyzing the use of facial recognition technology in all contexts.
-  **MS TEAMS** – Applied where content is at issue from Microsoft’s Teams collaboration platform.
-  **HYPERLINKED FILES** – These are links contained within an email, instant message or other format that direct a user to a related document. These occur in collaborative applications, chat platforms or web based email services like Google Mail and Microsoft Exchange online email. This issue is applied when the discovery of the data at these pointers or hyperlinks is requested, included in an ESI protocol, or analyzed by the court.

When a new issue tag is added to the database, our team conducts a review of all earlier decisions in the database and tags previous decisions that meet the criteria for that issue. Chart 3 below shows the total number of decisions in our database for each of the new issue tags added this year.

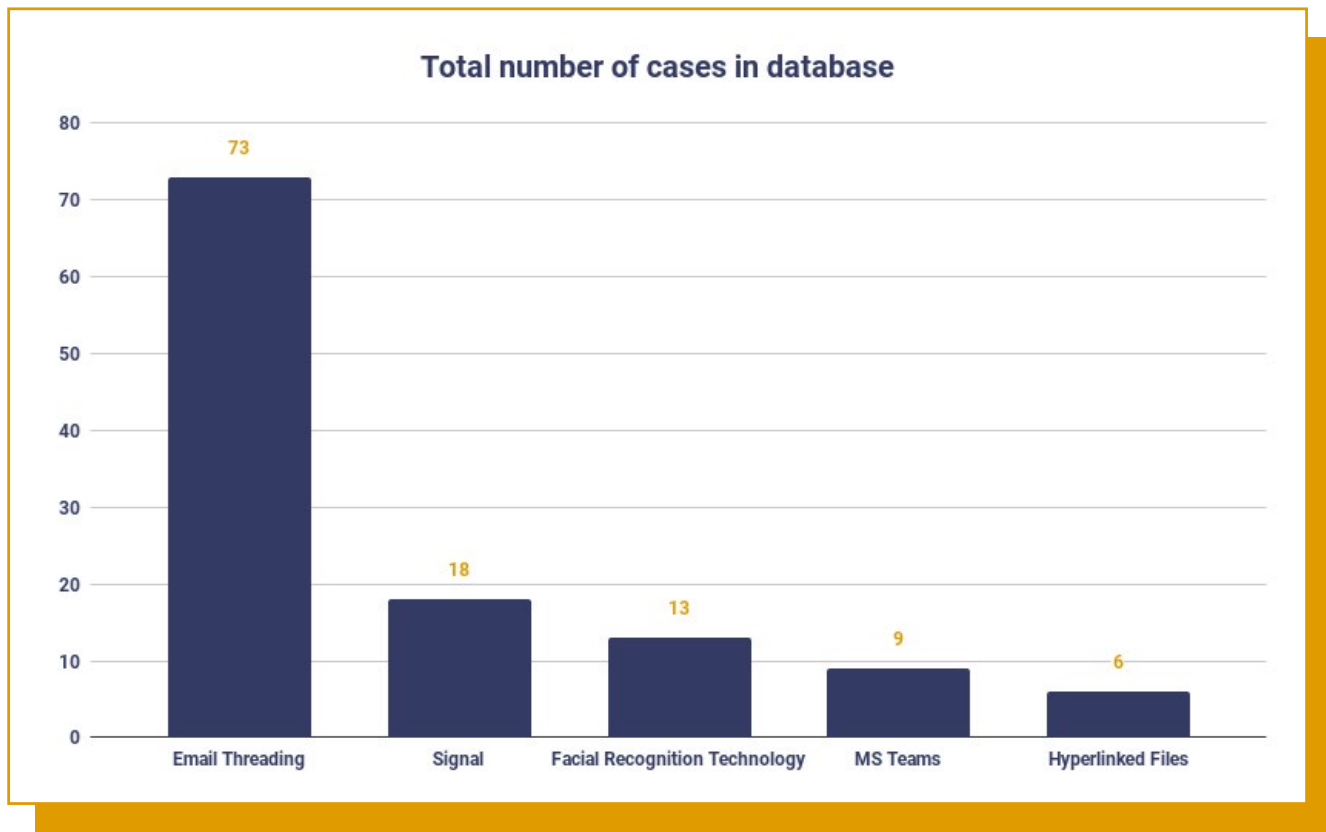


Chart 3 - New Issue Tags Added in 2023

Report Structure

This year our report focuses on an analysis of how specific issues are developing in the courts and is broken up into two parts: Takeaways from 2023 and Key Areas to Watch. 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. Key Areas to Watch include those issues we need to be paying attention to as they come before the courts for the impact they will have on ediscovery for parties and non-parties alike.

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 43 of the report provides an overview of our partners' technology or service offerings as well as a link to find out more information.

PART I: TAKEAWAYS FROM 2023

2023 brought significant developments in ediscovery case law, beginning with the sheer number of new decisions. At 5216 decisions, this past year is the largest number of decisions seen other than 2021 during Covid, when discovery disputes heard via Zoom drove up decisions by more than 20%.

Deep dives into the courts' decisions this year show several trends — a greater willingness to sanction parties for failure to follow the Federal Rules of Civil Procedure and their state equivalents, more detailed analysis on the capabilities of a party to provide relevant ESI from specific applications, and a string of cases holding parties to what they negotiate in their ESI protocols.

Sanctions under Rule 37(c) for Failure to Supplement Initial Disclosures

Since 2021, courts have held parties to task for their obligations to provide the data required under Rule 26(a) for initial disclosures, and for the failure to supplement under Rule 26(e). Those failures are now escalating into sanctions motions.

In [Beacon Navigation GmbH v. Bayerische Motoren Werke AG](#), BMW argued that Beacon should be sanctioned for its failure to produce source code as part of its initial disclosures or for the failure to supplement those disclosures under Rule 26(e). Beacon sued BMW for patent infringement on its vehicle navigation technology. BMW subcontracted to a third party company called Harman to build its technology. Due to a series of events, including BMW refusing to provide the source code claiming it did not have custody of it, Beacon did not subpoena Harman until 30 days before the close of discovery and did not receive the source code until after discovery had closed. Beacon did not produce the source code in discovery, but rather used the source code for the first time in its expert's report submission, after which BMW filed a motion for sanctions to exclude the source code as evidence for failure to disclose it during discovery.

Under Rule 37(c)(1), a party who fails to disclose information or identify a witness as required by Rule 26(a) or (e) “is not allowed to use that information or witness to supply evidence on a motion, at a hearing, or at a trial, unless the failure was substantially justified or is harmless.”

To guide the exclusion analysis under Rule 37(c)(1), the Sixth Circuit has adopted five factors for determining whether a party’s non-disclosure of evidence is substantially justified or harmless:

1. the surprise to the party against whom the evidence would be offered;
2. the ability of that party to cure the surprise;
3. the extent to which allowing the evidence would disrupt the trial;
4. the importance of the evidence; and
5. the non-disclosing party’s explanation for its failure to disclose the evidence.

The Court evaluated all five factors and found the first four factors weighed against exclusion. Notably, BMW was aware all along that Beacon would rely on the source code and could have provided it itself from Harman. The Court did find that Beacon’s excuse for delaying sending the subpoena lacked merit, although on balance, it did not change the Court’s mind, and the Court denied BMW’s motion for sanctions.

Counsel should heed the requirements of Rule 26(a) on initial disclosures and the duty to supplement under Rule 26(e). Savvy litigants will be watching for slip ups in this area and the case law is developing to allow for the exclusion of evidence or witnesses when failures meet the test under Rule 37(c)(1).

The Intent Requirement of Rule 37(e)

Since the amendments to the Federal Rules of Civil Procedure in 2015, few topics of conversation around them have been more extensive than the high bar required to meet the intent standard under Rule 37(e) to merit dispositive or terminating sanctions for failure to preserve. But case law in 2023 is starting to lower that bar and allow for adverse inference instructions and default judgment where there is no affirmative act or conspiracy to intend to destroy evidence – instead courts are finding intent based on the totality of the circumstances of a case.

In [Hunters Capital, LLC v. City of Seattle](#), plaintiffs were property owners who sued the City for damage to their property and businesses following the Capitol Hill Occupied Protests (CHOP) that arose in Seattle following the death of George Floyd in Minneapolis. On June 19, 2020, five days before the plaintiffs filed suit, the Seattle Mayor's office sent out a legal hold notice to its employees (but not to the Mayor) informing them of their responsibility to retain public records, such as text messages, on their city owned personal smartphones and mobile devices.

On June 24th, the plaintiffs also sent a letter to the Mayor advising the City of its obligations to preserve evidence, including text messages. On June 30th, the plaintiffs' counsel again sent another preservation letter to the City requesting preservation of text messages. After the plaintiffs filed the case, the Mayor, the Police Chief, and the Fire Department Chief, as well as six other individuals, deleted thousands of text messages from their mobile devices.

The facts of this case show a pattern of the City's failure to preserve data from mobile devices of key custodians. The Mayor, who was not on the list to receive the legal hold despite it being sent from her office, allegedly dropped her phone in the water on July 4th, and when restoring the phone once it started working, selected a "disable and delete" function that stopped synchronizing text messages with iCloud. She also took the active step to set all text messages to delete within 30 days causing the loss of 5746 text messages from prior to June 25.

The Police Chief was named in preservation letters but also did not receive a legal hold until July 27th. She resigned after CHOP and turned in her phone to the City in September 2020 but not before manually deleting more than 27,000 text messages from her phone, including everything before the date that she resigned.

The Fire Chief also did not receive a legal hold from the City until July 27th, and claimed he had no text messages prior to October 8, 2020, when he was locked out of his phone for using the wrong passcode too many times. He bought a new phone and had it reset by an employee at the Apple Store, deleting all prior text messages.

The Court addressed the analysis under Rule 37 as it applied to the facts on the plaintiffs' motion here and found that the text messages were ESI, that a substantial number of deleted texts were lost and cannot be restored or replaced, that the City did not take reasonable steps to preserve the text messages, and that its failure to preserve was "egregious."

The Court then considered, because those elements of Rule 37(e) are met, whether sanctions were appropriate, including whether the requisite intent and prejudice is established. As to prejudice, the court found that:

"Plaintiffs have been deprived of text messages from multiple officials representing the highest levels of City government and those responsible for establishing and implementing the City's response to CHOP. Of great significance is the fact that any direct messages between these officials, such as those between Mayor Durkin and Chief Best or between Mayor Durkin and Chief Scoggins, cannot be recovered. The Court finds that the deleted text messages threaten to interfere with the rightful decision in this case and sanctions against the City are clearly warranted."

As to intent, the Court noted "on this record, the court finds *substantial circumstantial evidence* that the City acted with the requisite intent necessary to impose a severe sanction and that the City's conduct exceeds gross negligence." (emphasis added.) All of the top ranking officials purged, through factory resets, changed retention settings, or manual deletions, thousands of CHOP related messages from their phones after they were under a clear obligation to preserve such information. The Court also pointed to the

"The ability to remotely collect a targeted set of data from a mobile device can mitigate substantial risk for organizations and counsel. These decisions granting sanctions for failure to preserve text messages highlight the difficulty in managing this process and the multiple steps of communication where preservation can get lost. This is one area where the technology is meeting the challenges presented as they arise."

– Matthew Rasmussen
Founder & CEO,
ModeOne

timing of the City's knowing about the Mayor's loss of text messages. The City knew about the Mayor's lost texts on August 21, 2020, shortly after the legal hold went out, but the City did not take any action to ensure that any other officials' text messages were preserved. The Court found that that was evidence of intent by the City under Rule 37(e).

In determining appropriate sanctions, the Court noted that although the plaintiffs had presented substantial circumstantial evidence that the City acted with the requisite intent to deprive, Plaintiffs have "not presented sufficient evidence from which the Court can conclude that the seven city officials acted pursuant to some elaborate conspiracy to delete their text messages." As such, the court granted an adverse inference instruction but refused to award terminating sanctions.

[Skanska USA Civil Se. Inc. v. Bagelheads, Inc.](#) is another case in which the defendant failed to preserve text messages from mobile devices after its duty to preserve had arisen. As in [Hunters Capital](#), the facts here illustrate with remarkable clarity the difficulty in preserving data from mobile devices and how quickly custodians and an administration can lose track of both the devices and the data on them. Skanska identified 13 custodians and ultimately had four of those custodians lose their cell phone data after turning their phones back into the company following the end of their employment. Company policy required resetting the phones to factory settings, and all data was lost from each of the devices. The fifth had his phone stolen out of his car with no backup in the cloud.

The Court's analysis found a "textbook case of spoliation" and that Skanska had specifically agreed in its ESI protocol to produce text messages from the named custodians. The Court noted that Skanska failed to suspend its normal document destruction procedures, failed to collect cell phone data from key custodians, failed to ensure its employees understood the litigation hold that they received, and failed to take any steps to prevent the destruction of cell phone data. While some of the text messages were included in the production of data from other custodians, the Court found that there was no dispute that there were text messages which are no longer available from any source.

Skanska tried to argue that it had just a gap in procedures and that any loss was inadvertent and not intentional, and that there was no prejudice to the claimants. The Court responded with this scathing quote:

“While the Court may be able to tolerate a gap here or there, the Court cannot ignore Skanska’s wholesale failure to take any steps to collect the cell phone data from these custodians or, at minimum, to ensure the custodians were aware of and understood the litigation hold that Skanska issued in October 2020. If the Court did not act to take some action in this case, it would, in essence, be rewarding Skanska for ignoring its preservation and collection obligations.”

Even without evidence of any affirmative act that was intentionally taken to deprive plaintiffs of evidence in the litigation, the Court found the requisite intent for sanctions under Rule 37(e) based on the bad faith standard. As to the appropriate sanctions, the Court imposed an adverse inference instruction, and rejected the notion that the case merited dismissal as that was a sanction of last resort.

Hunters Capital and Skanska are two high profile examples from extreme events where the courts effectively downgraded the affirmative act required for sanctions under Rule 37(e) to allow for a finding of bad faith where the facts warrant it and imposed adverse inference instructions.

Freeman v. Giuliani is a third example of the lowering standard of intent under Rule 37(e), but the first in which terminating sanctions have been issued. In a suit brought against him for defamation by two Georgia poll workers, Giuliani failed to preserve emails, text messages, WhatsApp messages and Signal data. Following multiple orders to compel production of discovery items, Giuliani failed to abide by the orders despite being given several opportunities by the Court, and plaintiffs moved for sanctions under Rule 37(e) seeking default judgment. Finding spoliation and prejudice, the Court held that “Giuliani’s failure to preserve his ESI has significantly prejudiced plaintiffs’ abilities to prove their claims because circumstantial

evidence of Giuliani’s knowledge of the falsity of his claims concerning plaintiffs likely would have existed in his lost ESI.” Analyzing Giuliani’s role as an attorney and that he admitted he fully understood his duty to preserve and was the sole person responsible for preservation, the Court found that he “intentionally and willfully ignored” his obligations and granted default judgment as a sanction for his discovery failures.

These three cases highlight a changing standard on the intent to deprive required under the amended Rule 37(e) and raise a red flag for counsel to properly advise on the duty to preserve and its scope early and often. With the lowered bar of bad faith or prejudice now sufficient for a finding of intent under that section, failure to take the proper steps may result in crippling or terminating sanctions.

Sources of ESI

Decisions in 2023 make it clear that it is more important than ever to ensure counsel and legal professionals supporting the ediscovery process know and understand the Sources of ESI at issue in a matter and work to preserve them quickly. To that end, early planning – information governance, creation of data maps, and creating a key list of sources for commonly occurring matters – is critical. As the decisions above reflect, courts are issuing more sanctions under FRCP 37(b)(2) and 37(C)(1) than in any year prior – and neither section requires a showing of intent or bad faith. Moreover, decisions demonstrating that the intent requirement of FRCP 37(e)(2) has been lowered mean that negligence in preservation may put parties square in the court’s crosshairs for adverse inference instructions and other crippling sanctions like the exclusion of evidence or witnesses.

“Mobile device forensics continue to present significant challenges in the eDiscovery landscape and increase the importance of planning and information governance initiatives. Recent issues like edited and unsent texts in iOS 16 Messages, identifying which attachments custodians actually accessed, and evolving privacy regulations impacting social media data collection pose significant hurdles. Organizations must proactively address these challenges by implementing and enforcing clear, defensible data policies that mitigate risk and ensure compliance.”

– Joey Seeber
CEO, Level Legal

This year also saw a huge uptick in data discovered from mobile devices as well as increased pressure from regulatory agencies on industries to preserve data in text messages and instant messaging applications as part of their compliance obligations. Agencies have levied [millions in fines](#) against companies for failure to comply. And while it’s just outside of 2023, in [January 2024 the FTC and DOJ](#) emphasized the importance of data from mobile devices by announcing that they are updating language in their standard preservation letters and specifications for all second

requests, voluntary access letters, and compulsory legal process, including grand jury subpoenas, to address the increased use of collaboration tools and ephemeral messaging platforms in the modern workplace. Per the announcement from FTC Bureau of Competition Director Henry Liu:

“These updates reinforce longstanding obligations requiring companies to preserve materials during the pendency of government investigations and litigation.

Companies and individuals have a legal responsibility to preserve documents when involved in government investigations or litigation in order to promote efficient and effective enforcement that protects the American public. Today’s update reinforces that this preservation responsibility applies to new methods of collaboration and information sharing tools, even including tools that allow for messages to disappear via ephemeral messaging capabilities.

These updates to our legal process will ensure that neither opposing counsel nor their clients can feign ignorance when their clients or companies choose to conduct business through ephemeral messages... The Antitrust Division and the Federal Trade Commission expect that opposing counsel will preserve and produce any and all responsive documents, including data from ephemeral messaging applications designed to hide evidence. Failure to produce such documents may result in obstruction of justice charges.”

In short, and as many of the decisions in this 2023 Case Law Report will highlight, we are past the days of wiggle room and claiming negligence in failing to meet your discovery obligations. Courts are holding all parties to the letter of the law. Negotiate your ESI protocols only after having a full understanding of your sources of ESI and what you may be required to produce. Revisit your policies on mobile devices, keeping in mind that courts’ analysis as to the discoverability of data on them is more about whether relevant data exists than whether the company or individual owns or pays for the device. Courts are looking sharply at the language of the Rules and, for what seems to be the first time, deciding when the language does not fit the complexities of ESI and tailoring sanctions to the totality of the circumstances. Arguments seeking to couch ESI issues in hard copy documents will not carry the day.

The sections below address how courts are addressing the most prominent issues in case law decisions from 2023 including hyperlinked files, Signal, Slack, Microsoft Teams and video.

Hyperlinked Files

Last year's report identified this issue as a Key Area to Watch and we anticipate it will be again for 2024. 2023 did not bring any developments or consensus on the language to be used in discussing this issue of when a link to a document is included in an email or message vs. having the physical document attached. Links to what used to be physically attached to an email are problematic for several reasons, among them:

- **Version Control** – that collection must consider which version of the document was at the link when the message was sent,
- **Location of the Document at the Link** – i.e. whether the document at the link has been deleted or moved,
- **Creating the Parent/Child Relationship** – the tools used for collection must capture the document at the link and create a metadata field to ensure the parent/child relationship can be maintained (if agreed upon between the parties), and
- **Reporting** – whether any report can be created of documents that are not captured and why.

Recall that Judge Parker's decision in [Nichols v. Noom Inc.](#) from 2021 declined to require Noom to reproduce documents that did not include the linked files as attachments, holding that not all hyperlinks are attachments, and distinguishing between links to websites vs. actual links to documents. Key to Judge Parker's analysis in that matter was that Noom had already produced documents from Google Suite based on the parties' agreement.

Since [Noom](#), no court has addressed the thorny language or production issues, instead relying on the parties to negotiate how they will be handled in the context of their ESI protocols.

The first decision of the year came in the form of the negotiated ESI protocol entered as an order in [In re Acetaminophen – ASD-ADHD Prods. Liab. Litig.](#) on January 17, 2023. In that decision, the parties agreed to the following language treating linked documents *as traditional family relationships* and requiring them to be collected and produced with the parent message and to provide metadata fields identifying the linked document as an attachment:

19. Parent-Child Relationships. Parent-child relationships (association between an attachment and its parent document) shall be preserved. The attachment(s) shall be produced adjacent to the parent document, in terms of Bates numbers, with the first attachment being named with the next sequential number after the parent, and any additional attachment(s) sequentially numbered after that first attachment. Email attachments and embedded files or “modern attachments” (i.e., hyperlinks pointing to files stored in the cloud or a shared repository such as SharePoint and other types of collaborative data sources, instead of being directly attached to a message as has been historically common with email communications) shall be collected and produced with the parent message. “PRODBEGATT” and “PRODENDATT” fields listing the unique beginning Bates number of the parent documents and ending number of the last attachment must be populated for each child and parent document.

Three months later, in [In re StubHub Refund Litig.](#), United States Magistrate Judge Thomas Hixson ruled on a motion to compel after StubHub failed to produce documents from the links in emails. The Court required StubHub to meet its production obligations under the parties' agreed upon ESI protocol entered as an order that included the following technical specifications for the production of hyperlinked documents:

“Email repositories, also known as email databases (e.g., Outlook .PST, Lotus .NSF), can contain a variety of items, including messages, calendars, contacts, tasks, etc. *For purposes of production, responsive items should include* the ‘Email’ metadata/database fields outlined in the Metadata Table, including but not limited to all parent items (mail, calendar, contacts, tasks, notes, etc.) *and child files* (attachments of files to email, *hyperlinks to internal or nonpublic documents*, or other items), with the parent/child relationship preserved. Similar items found and collected outside an email repository (e.g., .MSG, .EML, .HTM, .MHT) should be produced in the same manner.”

“*A document and all other documents in its attachment range, emails with attachments, and email or other documents together with any documents referenced by document stubs or via links to internal document sources within those emails or other documents all constitute family groups. If any member of a family group is produced, all members of that group must also be produced or else logged as privileged, and no such member shall be withheld from production as a duplicate.*” *Id.* (emphasis added). “Hyperlinked files must be produced as separate, attached documents.”

Despite that language, StubHub produced emails and attachments from Google Suite separately, not as attachments. The court distinguished [Noom](#) and held StubHub to its obligations, noting that it had not moved to amend the order:

“Litigants should figure out what they are able to do before they enter into an agreement to do something. Litigants should live up to their agreements, especially when they are embodied in court orders, as the ESI Protocol is here. And if for some reason, a party learns that a so-ordered discovery agreement has become impossible to comply with, the party should promptly move for relief, with a good showing that despite its best efforts, compliance is impossible. In this case, StubHub has decided to do ‘none of the above.’ Its document production is in violation of the ESI Protocol, StubHub hasn’t done everything it could, it hasn’t moved for relief from the protocol, and it hasn’t settled on a clear story for why producing the linked documents can’t be done.”

The parties did not agree on the production of hyperlinked documents and sought court intervention in [In re Meta Pixel Healthcare Litig.](#) In that decision, United States Magistrate Judge [Virginia DeMarchi](#) addressed a disagreement over the language of the parties’ proposed ESI protocol on linked documents. After reviewing affidavits from Meta that argued being required to collect documents at hyperlinks even using Microsoft’s built in Purview tool “would disrupt Meta’s standardized workflow for ESI-related discovery processing across all of its platforms and systems”, the Court held that hyperlinked documents should not be treated as conventional attachments but advised the parties to consider the issue on a “case-by-case” basis:

“The Court is persuaded that the commercially available tools plaintiffs suggest may be used for automatically collecting links to non-public documents have no or very limited utility in Meta’s data environments or systems, and even that limited utility (i.e. using the Microsoft Purview eDiscovery (Premium) tool to collect links to SharePoint and OneDrive cloud attachments in Microsoft Exchange environments) would disrupt Meta’s standardized workflow for ESI-related discovery processing across all of its platforms and systems. Accordingly, the ESI protocol should make clear that hyperlinked documents are not treated as conventional attachments for purposes of preserving a “family” relationship in production. However, the Court anticipates that for some documents, it will be important to collect (or attempt to collect) hyperlinked documents

and associate them with the underlying ESI in which the links appear. In such circumstances, the parties should consider reasonable requests for production of hyperlinked documents on a case-by-case basis. Such requests should not be made as a matter of routine.”

While three decisions do not make up a body of law, the trend we are seeing on this issue is that parties need to understand how the platforms they use allow users to create and store documents at hyperlinks that are discoverable and how they will collect them before agreeing to language that obligates them beyond their capabilities. This is consistent with the theme of needing to fully understand the technical issues inherent in the sources of discoverable ESI before signing off on an ESI protocol. As discussed below and highlighted in the quote from Judge Hixson, courts are holding parties to what they agree to in a protocol.

In lieu of consensus language around this issue, we created the Issue Tag titled “Hyperlinked Files” in eDiscovery Assistant to identify these issues. Currently, [seven decisions](#) in our database include the Issue Tag, the three decisions discussed above as well as the [Noom](#) decisions and [IQVIA, Inc. v. Veeva Systems, Inc.](#)



Changes to the platforms that allow links to documents to be shared vs. physically attached theoretically may help to alleviate this ediscovery challenge. In an update [released December 5, 2023](#), Google announced that:

“Starting December 8, 2023, admins can export Drive files hyperlinked in Gmail messages directly in Google Vault. When admins select “export linked Drive files”, Vault will look for Drive hyperlinks in the body of the emails being exported from Gmail. If Drive hyperlinks are found, a separate export of Drive files will also be created.

Admins will be able to find their exported hyperlinked Drive content nested under the corresponding Gmail export in the “Export” tab. Vault admins can find the association between the Gmail export and Drive link export in the export file names and metadata.”

Similarly, Microsoft [announced in October 2023](#) that customers with an E5 license could leverage new functionality in Purview:

“To address this challenge, eDiscovery (Premium) provides two solutions for collecting cloud attachments:

-  Collecting the live version of a document that is linked to in a cloud attachment.
-  Collecting the version of the document at the time it was shared in a cloud attachment.

When you create a collection estimate and the search results contain items that include cloud attachments, you have the option of collecting the target of the cloud attachment when you commit the collection estimate to a review set. When you select this option, eDiscovery (Premium) adds the documents that are linked to in the cloud attachment to the review set. This allows you to review the target documents and determine if the document is relevant to your case or investigation.”

We’ll keep an eye on this issue as it evolves, and whether these changes or the continued development of technology makes the collection and production of hyperlinked files a non-issue moving forward. Bear in mind that technologists testing these tools have found that the issues noted above still persist.

Signal

Data from the instant messaging platform Signal was at issue in [ten decisions in 2023](#), bringing the [total decisions to 18](#) and solidifying it as a key source of ESI that counsel need to be aware of and understand how it works.

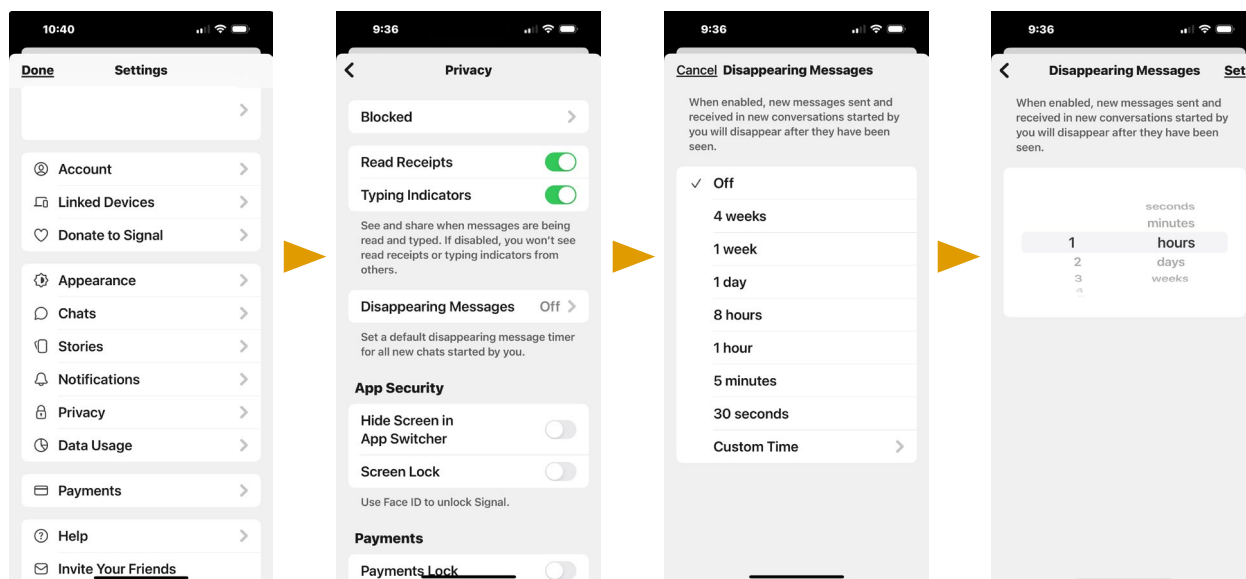
Two weeks into 2023, in the [Hunters Capital v. City of Seattle](#) case discussed above, the Court rejected the City’s argument that plaintiffs failed to preserve messages in Signal, finding that although not all messages were available from plaintiffs’ phones, more than 8866 Signal messages were made available from a third party who participated in the “neighborhood chat” at issue and the plaintiffs could not recall sending any other messages via the application.

Interestingly, in that case, the Court noted that “Signal is known for ‘disappearing messages’,” which can be automatically erased from every participant’s phone after a period set by the sender. And, while disappearing messages were not at issue in [Hunters Capital](#) because the plaintiffs did not utilize the functionality, it was a key issue two weeks later in [U.S. v. Bankman-Fried](#).

In that case, the government sought to modify the release conditions of defendant Samuel Bankman-Fried, the former CEO of FTX who had been arrested on multiple fraud and money laundering charges tied to the collapse of FTX and its sister hedge fund Alameda. The government sought to preclude Bankman-Fried from communicating with any current or former employees of either entity or using any encrypted or ephemeral call or messaging application, including, but not limited to Signal.

In support of its position, there was no dispute that Bankman-Fried had directed that FTX and Alameda business be conducted on both Slack and Signal and that messages on the platforms be set to automatically delete after 30 days or less. The factual proffers by the government were sufficient to modify the release conditions to preclude communication via any encrypted or ephemeral call or messaging applications, including Signal.

Counsel need to understand how Signal works. Signal is an encrypted messaging application available only for mobile devices — there is no desktop application. Data created, sent, received and stored in Signal is only available on the sender or recipient’s mobile device. While both Slack and Signal allow for the user to adjust settings to automatically delete after a period of time, those settings are not on by default. A user must take conscious steps to change the settings. The screenshots below from the most current version of Signal on an iPhone show the process a user must go through to make messages ephemeral – also described by the courts as disappearing messages. The process, which was modified with the most recent update of Signal requires the user to click through Settings ► Privacy ► Disappearing Messages to create their own timing for messages to disappear:



Additional decisions from the year further emphasize the importance of understanding how custodians are using Signal and how quickly action needs to be taken to preserve ESI stored in the application. Data from Signal was also at issue in [Freeman v. Giuliani](#), in which the court found that Giuliani failed to preserve messages from Signal and WhatsApp.

In [McConnell v. Advantest Am., Inc.](#), the California Court of Appeals held that the California Arbitration Act gave the arbitrator power to issue a subpoena that included documents from Signal, Telegram, Wickr, WeChat, WhatsApp, text messages or “any other messaging service or platform relating to” the business at issue.

In [Barak v. Rooster’s Guide & Outfitting Adventures](#), the Court denied plaintiffs’ argument seeking an adverse inference instruction for the alleged spoliation of Signal messages where there was no bad faith or intent to deprive and more than 2700 messages were provided to plaintiffs in discovery.

Decisions from 2023 make it clear that data from Signal is subject to all of the obligations under the Federal Rules of Civil Procedure and that counsel’s obligations include understanding how the application works and that the ephemeral functionality in the app requires early intervention to preclude preservation issues.



Like Signal, decisions on data from the Slack platform ramped up in 2023, adding [seven new decisions](#) in which courts weighed in on issues in discovery data from the collaboration tool. In [FTC v. Am. Future Sys., Inc.](#), the court ordered the production of eight years of Slack data from July 1, 2015 to the present (decision dated May 17, 2023) from four different workspaces using previously negotiated search terms.

United States Magistrate Judge Armstrong’s decision in [Lubrizol Corp. v. IBM Corp.](#) includes important takeaways about context in identifying responsive Slack messages when search terms are applied. The dispute began when IBM failed to produce complete conversation threads from Slack and Lubrizol sought the full threads. The parties negotiated and Lubrizol amended its request from complete threads to requesting (1) that, for any Slack conversation containing 20 total messages or fewer, IBM be required to produce the entire conversation, so long as the conversation contains at least one responsive message; and (2) that, for any Slack conversation containing more than 20 total messages, IBM be required to

produce the 10 messages preceding and following any responsive message. IBM opposed the proposal, arguing that it had already reviewed the Slack messages hitting on the agreed upon search terms as well as the ten messages before and after the responsive term, and that it had produced any responsive messages within that ten message window that provided context. Any additional production, it claimed, was unduly burdensome and not proportional to the needs of the case.

Magistrate Judge Armstrong began her analysis by acknowledging that the question of whether to treat Slack messages as individual documents whose relevance must be analyzed separately was one of first impression. She rejected IBM's argument that contextual production was the equivalent of producing irrelevant hard copy documents, and found that each Slack message should be treated like a separate document. Instead, the Court found that Slack messages are more akin to text messages than hard copy documents and went on to evaluate multiple other rulings from courts in determining the appropriate context. Following an analysis that production was not burdensome, that there was a legitimate dispute about the relevance of the withheld messages, and that a protective order decreased concerns regarding sensitive irrelevant messages, the Court accepted Lubrizol's proposal requiring IBM to produce (1) the entirety of any Slack conversation containing 20 or fewer total messages that has at least one responsive message; and (2) the 10 messages preceding or following any responsive Slack message in a Slack channel containing more than 20 total messages.

Lubrizol is instructive in that parties with matters in which Slack or other collaboration platform data is implicated will need to consider context for production early in the matter.

Microsoft Teams

2023 marked the first time case law directly addressed Microsoft Teams data. The Court in [Turtle Mountain Band of Chippewa Indians v. Howe](#) is the first decision to note the discoverability of Teams data.

Four of the [eight decisions this year](#) came from the [Deal Genius v. O2Cool, LLC](#) matter. Following disputes related to the production of emails from Microsoft 365, the Court appointed a Special Master. In his [initial Report](#), the Special Master noted what many ediscovery professionals have long known - that “the Microsoft 365 platform is replete with deficiencies that may prevent a responding party like Deal Genius from generating reliable search results and thus satisfying the Rule 26(g)(1) reasonable inquiry standard.” And in paragraph 14 of his Report, the Special Master expressed concern over Deal Genius’ delay in producing Teams messages despite requests that required responsive messages served more than 18 months prior:

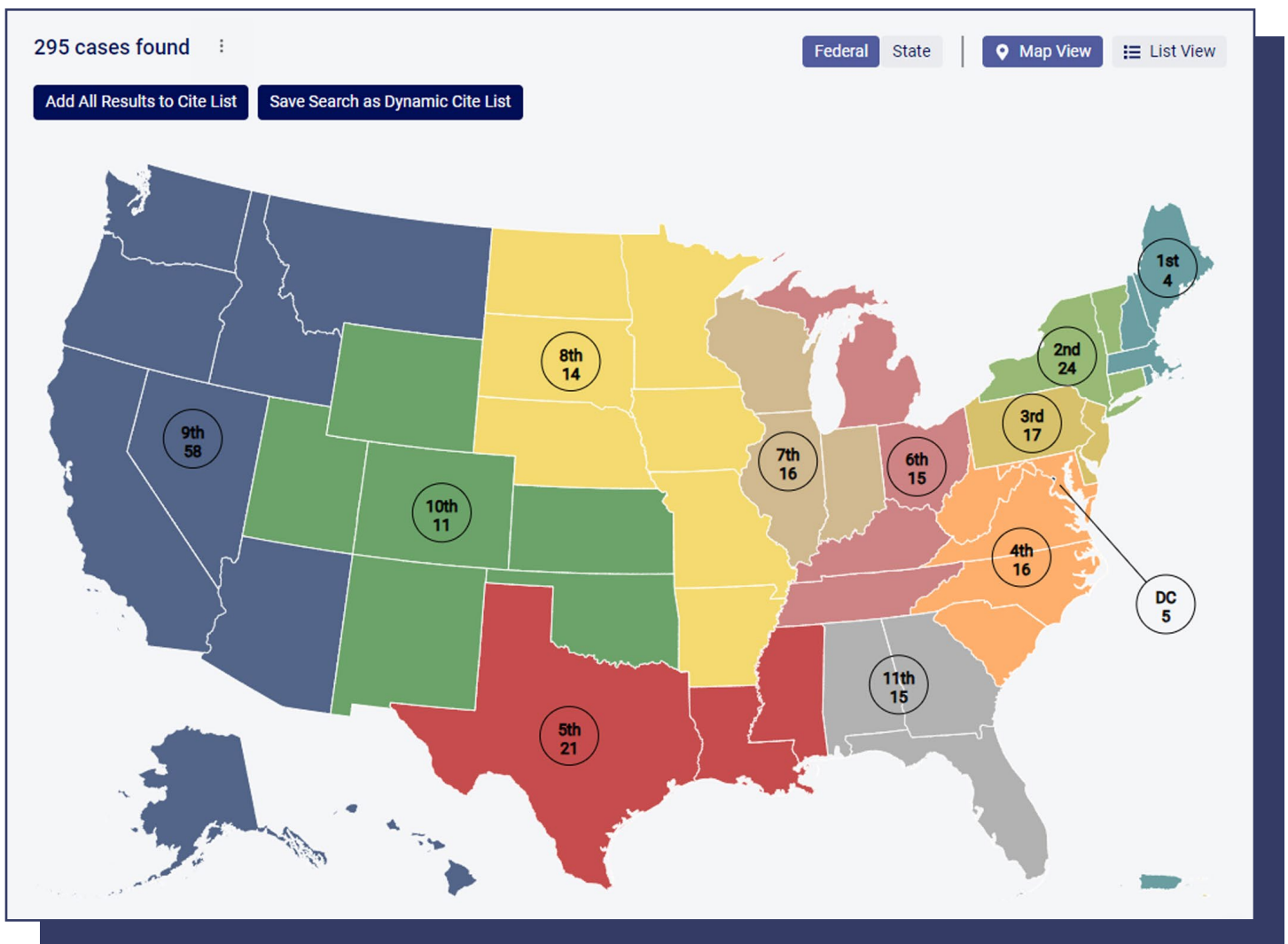
“That Deal Genius may have overlooked, ignored, or withheld responsive Teams messages in discovery raises serious concerns and the Special Master RECOMMENDS further inquiry into this aspect of Deal Genius’s discovery conduct. Failure to conduct a reasonable search or permit discovery of relevant information may justify the imposition of severe discovery sanctions.”

O2COOL then raised concerns about “emails” produced that did not appear to be emails, only to learn at the hearing from Deal Genius that the documents in question were not emails but stand alone messages from Teams produced by Deal Genius. The Special Master granted O2COOL’s request and ordered Deal Genius to produce additional Microsoft Teams messages exchanged on the same communication string on the day the communications at issue took place, along with the preceding and following days. The Special Master permitted Deal Genius to redact irrelevant messages from the Microsoft Teams messages while admonishing Deal Genius not to produce message strings replete with redactions.

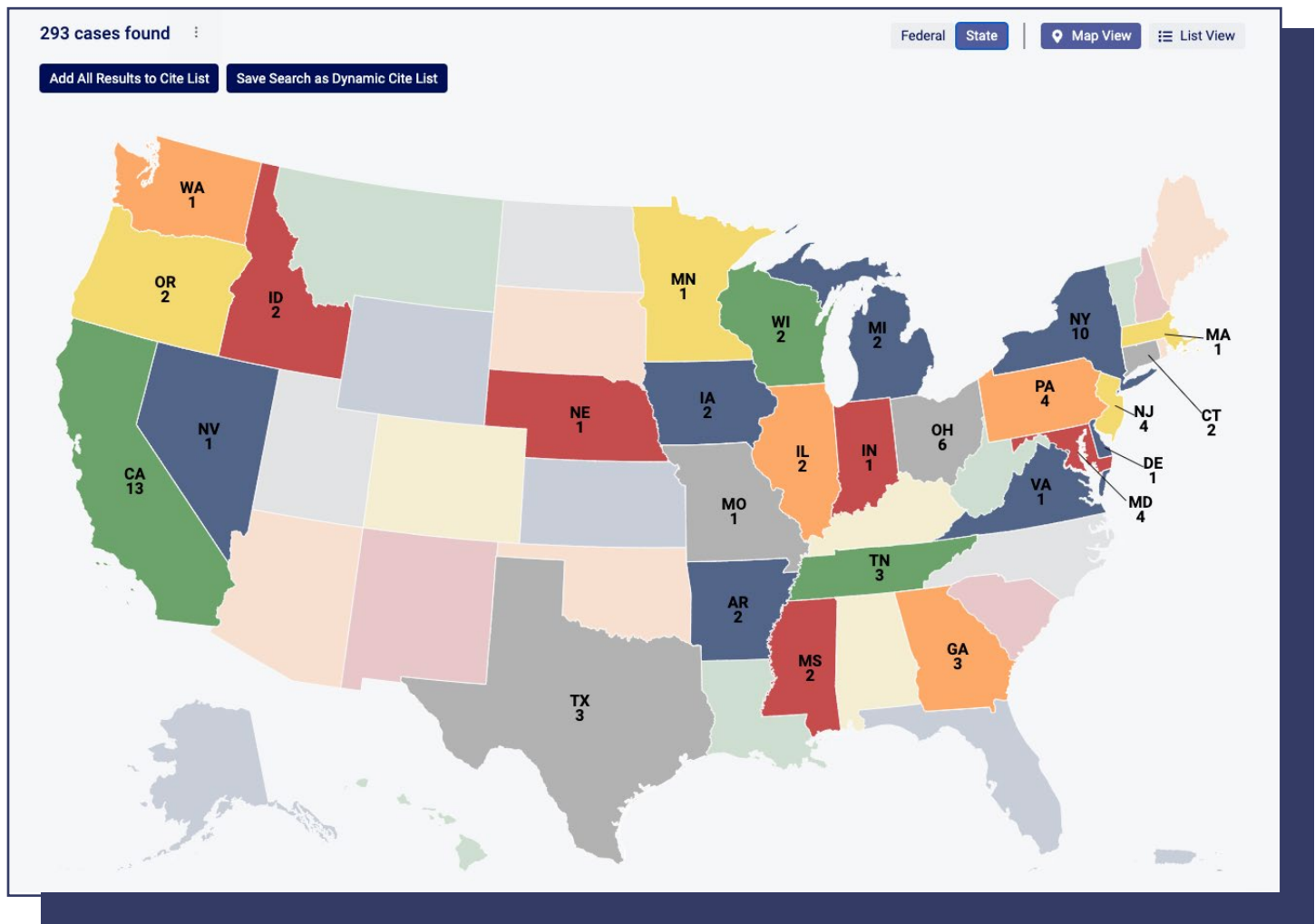
The [Deal Genius](#) decisions confirm both the discoverability of data from Microsoft Teams and illustrate that the context issues raised in [Lubrizol](#) about Slack messages are also relevant to Teams data. Counsel will need to consider the context issue early in planning for matters and conduct data analysis to be able to propose 1) an appropriate time period for relevant data, 2) search terms to locate relevant messages, and 3) the amount of context (i.e. number of messages or time delineation) that should be provided to meet counsel’s obligations under Rule 26.

Video

Of the 5216 decisions this year, [295 raised issues](#) involving the discovery of video data. Maps 3 and 4 below show the wide ranging distribution of cases from every federal circuit and 26 different states. Judges across the country are comfortable with the discovery of these data types and will not hesitate to impose sanctions for the failure to preserve relevant data.



Map 3 - Decisions Involving Video in Federal Courts in 2023



Map 4 - Decisions Involving Video in State Courts in 2023

One such example is the failure to preserve video at a retail location of Rite Aid that led to an adverse inference instruction, judgment in favor of the plaintiff in excess of \$230,000, and an affirmation on appeal in [Aposaga v. Rite Aid Corp.](#) As covered on [Episode 121 of the Case of the Week](#), Plaintiff alleged she slipped and fell on a substance in an aisle resulting in significant, disabling injuries. At the time of the incident, the Rite Aid store in question had video cameras that were turned on and would have captured the plaintiff walking into the store, as well as walking to the aisle where the Benadryl that she was buying would have been located. According to the Court, the video of plaintiff walking in would have shown whether she had

any issues with walking that might have supported Rite Aid's argument that she lost her balance, and that the video of her walking between the aisles would have resolved the disagreement over where she fell.

Rite Aid argued on appeal that the admission of the preservation letter from counsel, sent thirteen days after the event, was improperly admitted into evidence, and that without the letter, there was no evidence to support giving the jury instruction. Rite Aid argued that the preservation letter was not legally sufficient to impose a duty to preserve the video because it did not specifically, "explain why video for the entire day for the entire store was relevant."

"Video represents powerful, built in storytelling and is some of the best evidence available. However, managing video for compliance and ediscovery can be a logistical nightmare due to the overwhelming volume that routine capture represents. Meeting legal obligations for the preservation of video requires specific, careful coordination between those who are operationally responsible for the system and the legal and compliance departments."

– Joy Murao
Founder and CEO
Practice Aligned Resources

The Court disagreed and found the letter was sufficient to impose a duty to preserve on Rite Aid and that the video would have been relevant to the facts at issue. The Court also included some language that is very important for clients who have retail storefronts where this issue may occur in California and in any jurisdiction that adopts the holding here:

"It should go without saying that direct evidence of a plaintiff falling or the spot where she fell is not the only relevant evidence in a personal injury action. A store owner has a duty to exercise ordinary care and does so by making reasonable inspections of the portions of the premises open to customers. Thus, at a minimum, a pattern of regular maintenance of the interior of a business open to the public plays an

important role in defending against claims for personal injury by customers. In addition, while a customer's ability to walk may not be an issue in every personal injury case, it is certainly a common issue across a variety of businesses. Rite Aid knew or should have known that any video showing inspections or maintenance of the store aisles or showing that plaintiff had difficulty walking would be relevant."

The Court found that the video existed, should have been preserved, and that after being asked to preserve the video, Rite Aid, "chose to destroy the video." The Court noted that:

"the relevance of videos and other parts of the store was readily apparent from the bare fact of plaintiff's slip and fall. These facts are more than sufficient to support an inference that Rite Aid destroyed the video to prevent it from being used in litigation. We find it particularly telling that Rite Aid did not preserve even the one piece of video which indisputably would have shown plaintiff in the store, the video of her walking into the store. Without this video, Rite Aid could, and did, remind the jury that plaintiff had neuropathy, which causes pain, balance problems, numbness in the feet, thereby suggesting that the neuropathy was the reason she fell."

Three additional decisions are worthy of noting on the failure to preserve video evidence:

- In [Rapp v. Naphcare, Inc.](#), Washington District Judge David G. Estudillo granted the plaintiff's motion for sanctions, issuing a default judgment against Kitsap County in Washington for spoliation of video evidence related to the suicide of an inmate in the Kitsap County Jail.
- In [Bourell v. Ronscavage](#), Connecticut Magistrate Judge Maria E. Garcia used the six proportionality factors of FRCP Rule 26(b)(1) to determine that the plaintiff must produce video journals depicting the plaintiff's injuries, symptoms, and recovery, following the accident that was the subject of the lawsuit.

In [Castro v. Smith](#), New York District Judge Jessica G. L. Clarke, while finding that defendants did not act with intent to deprive, ruled that the plaintiff was allowed to present evidence that video footage existed that would have shown, at a minimum, the aftermath of an incident with the New York City Department of Corrections (“DOC”) where the plaintiff was hit in the face.

The dramatic uptick in decisions involving video evidence this year make it abundantly clear that organizations need to prioritize policies and governance around video evidence. The burden placed on organizations will be high, but decisions in 2023 show that courts are holding parties accountable and getting out in front allows for considerable risk mitigation.

ESI protocols

One of the overriding themes of decisions from 2023 was that courts will hold parties to what they agree to in an ESI protocol. Once entered as an order, an ESI protocol has all the power of any court order, and can serve as the basis for sanctions if violated under Rule 37(b)(2). Several cases demonstrate the need to know your data before entering into a protocol that may saddle you with more obligations than you can meet.

Covered earlier in the Hyperlinked Files section of this Report, in [In re StubHub Refund Litig.](#), California Magistrate Judge Thomas S. Hixson granted the plaintiffs’ motion to compel and ordered the defendant to produce the linked documents as agreed to in the ESI protocol or “produce for deposition within 14 days after the deadline to complete document production a Rule 30(b)(6) witness with full knowledge of everything StubHub and its vendors did in attempting to produce linked documents as attachments as required by the ESI Protocol.”

In its protocol, StubHub agreed to produce linked documents within its collection, but failed to do so and offered multiple reasons to the Court, none of which were persuasive. Judge Hixson’s quote, below, sums up his position and is consistent with other decisions on this issue:

“This order is about agreements. Without them, courts would have to rule on everything, and litigation would be even more expensive than it already is. Courts encourage parties to work out things like ESI protocols and procedures governing discovery. We do this because we assume that the parties have some idea what they want to obtain in discovery, they know much better than the Court does what is possible or feasible, and they are best able to estimate the costs involved in whatever they agree to do. And when parties reach an agreement, we ordinarily need to hold them to it. Otherwise, if discovery agreements routinely turn out to be worthless and unenforceable, we deprive the parties of any reason to enter into them.”

Similarly, in [Latin Markets Brazil, LLC v. McArdle](#), plaintiffs agreed not to seek voicemails, text messages, personal phones or tablets in an ESI stipulation, but then learned that the best evidence they needed lived in text messages exchanged by the other side. New York Supreme Court Justice Robert R. Reed denied the plaintiff’s request for texts, social media, and LinkedIn messages based entirely on the earlier agreement.

The debate rages on about the effectiveness of an ESI protocol where one side uses it as a weapon to seek far greater certainty in ESI issues than can be hoped to achieve and creates a months long dispute over the agreement. These cases, and [dozens of others from 2023](#), demonstrate clearly that having a protocol can be a blessing and a curse. To keep it in the blessing category, understand your data sources and your ability to meet the obligations you agree to before entering into them, or seek redress from the court when issues arise that mean obligations cannot be met.

Earlier in 2023, eDiscovery Assistant produced a practical Guide titled [Drafting a Thoughtful ESI protocol](#) that addresses many of the issues raised by the decisions in 2023 and lays out the details to be considered for each. You can download that guide [here](#).

PART II: KEY AREAS TO WATCH

Last Year's Areas to Watch – What Happened?

In last year's areas to watch we identified mobile device discovery and emojis as two potential areas for development. Mobile device discovery, framed more in sanctions for failure to preserve text messages and Signal data, exploded in 2023 and proves to be even bigger in 2024 with the new regulatory requirements just issued in January 2024. We also anticipate seeing more clarity from the courts on possession, custody and control of mobile devices as they determine whether that requirement of Rule 34 must exist to require discovery of a mobile device that contains relevant, discoverable evidence. In [Miramontes v. Peraton, Inc.](#), the Court rejected the idea an employer only has “control” over its employees’ communications if it has a legal right to obtain them on demand:

“While this bright-line test has intuitive appeal, the realities of modern business require a fact-specific approach. Today, many, if not most, employees use cell phones for work. And while some companies issue work devices, others, including Peraton, do not. Under Peraton’s view, a company could effectively shield a significant amount of its employees’ business communications from discovery simply by allowing its employees to conduct business on their personal phones. For these reasons, the Court agrees with other courts that have found electronically stored information on employees’ personal devices may be under the control of their employer in certain circumstances.”

Case law involving emojis emerged as predicted, with [four rulings citing interpretation of emojis](#) as critical to a ruling. In [In re Bed Bath & Beyond Corp. Sec. Litig.](#), the Court interpreted the defendant’s use of the smiley moon emoji as telling his hundreds of thousands of followers on Twitter that Bed Bath’s stock was going up and that they should buy or hold.

Looking Towards 2024

Technological advancements, generative AI, and proposed amendments to the Federal Rules of Civil Procedure regarding privilege logs lay the groundwork for another record breaking year in ediscovery case law in 2024. 2023 brought about a level of sophistication in decisions from courts on complex issues that we have not seen as consistently before, and that will likely increase in 2024. With budget constraints and outside counsel costs escalating, the time is now for organizations and counsel to collaborate on how to mitigate risk in preservation, collection and production of ESI.

Privilege Logs

Lawyers and legal support professionals all over the country have become frustrated by the effort and cost associated with the creation of a privilege log to meet the requirements of Federal Rule of Civil Procedure 26(b)(5)(A). Large cases make the creation of privilege logs an onerous and complicated process, and some courts have begun [to allow the use](#) of categorical privilege logs or [enforce them](#) when the parties agree to use them as part of their ESI protocol.

New York State Courts have been advising the use of categorical privilege logs since 2014 when the Commercial Division of the Supreme Court of New York adopted [Rule 11-b of Section 202.70\(g\)](#). The [New York City Bar Committee on State Courts of Superior Jurisdiction](#) recently released guidance “useful for parties who may be new to the concept but whose cases may warrant a departure from the traditional document-by-document privilege log.”

The cost of privilege logs has also spurred activity and proposed amendments to the Federal Rules of Civil Procedure. The Advisory

Committee on Civil Rules has [proposed amendments to Federal Rules of Civil Procedure 26\(f\)\(3\) and 16\(b\)\(3\)](#) which require the parties to discuss the timing and method for complying with Rule 26(b)(5)(A) related to privilege claims. The proposed Committee Notes note that compliance with Rule 26(b)(5)(A) can “involve very large costs” and suggests that “in some cases” it may be suitable for a document-by-document analysis without an explanation of the grounds for withholding or for “some sort of categorical approach.” The Committee held a hearing on January 16, 2023, and the proposed amendments are set for publication on December 1, 2025, following enactment by The Supreme Court and Congress.

Predictions

With the level of technological development already underway, the near complete adoption of the cloud, and continued privacy issues, we expect to see the following in 2024:

- Shorter and more thoughtfully negotiated ESI protocols
- Initial continued fumbling with hyperlinked files and the family relationship status until the technology allowing users to create them allows for appropriate ediscovery collection
- Case law associated with content created using generative AI, particularly deep fakes
- Additional decisions following on the court’s ruling in [Miramontes](#) as to whether the possession, custody or control standard of Rule 34 is required to make relevant information on the personal mobile device of an employee who uses it for work discoverable
- An even greater use of text and instant messaging applications by employees to communicate
- Organizations taking additional information governance steps to prepare for the discovery of data on mobile devices and to reduce risk in the overall volume of information available

We will continue to cover the evolution of these issues on our [blog](#) at eDiscovery Assistant, and our [Case of the Week series](#).

Conclusion

The overwhelming takeaway from this past year is the need, now more than ever, for organizations to understand how and what sources of ESI are being used to conduct business and have a plan for preserving, collecting and producing them. There simply will not be enough time to figure it out once litigation has arisen, and recent decisions show the courts' desire to hold parties accountable for meeting those obligations even when there is no evidence of active intent to destroy data. Conducting an assessment tailored to what your organization or client's litigation or risk portfolio looks like and creating a data map or structure of often implicated data sources is the place to start. That assessment will then lay the foundation for where to proceed in records management and help you identify technology needs to assist with the pain points.

There is no question that the way we do business has changed. The shift to mobile devices began pre-Covid, and has steamrolled with the widespread adoption and use of collaboration platforms like Teams and Slack. Regulatory agencies are moving faster than ever to require industries to meet compliance requirements for data only stored on mobile devices. Technology is working hard to keep pace and stay ahead of those requirements, but lags behind. Simply put, the systems that we use to create, store, send and receive data are not built to go and find relevant data for investigation or litigation purposes.

For the first time in decades of following ediscovery case law, we are seeing proactive decision making from courts in which they are looking at the sum total of the conduct against a party's obligations under the governing rules and finding bad faith and prejudice are sufficient to award harsh sanctions including the exclusion of evidence or witnesses, adverse inference instructions and default judgment. Case law from 2023 is clear on our obligations as counsel — whether you heed those obligations rests with you.

Acknowledgements

We would like to express our deepest appreciation to our Partners for their invaluable support in helping us bring the 2023 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

eDiscovery Assistant empowers lawyers and legal professionals to harness the power of Electronically Stored Information (ESI) with confidence. Our platform provides a curated database of case law, rules, resources, and on-demand ediscovery education, all meticulously tagged for fast, issue-based searching. Go beyond traditional research and gain instant insights with AI-generated summaries and actionable checklists.

Go beyond just case law:

- ✓ **Stay informed:** Access hundreds of new case decisions weekly, tagged for specific ediscovery issues.
- ✓ **Navigate the rules:** Easily reference all relevant ediscovery rules from various U.S. jurisdictions.
- ✓ **Gain clarity:** Visualize and understand key issues with our interactive dashboard and unique tagging system.
- ✓ **Work smarter:** Utilize actionable checklists, forms, and AI-generated case summaries.
- ✓ **Learn on the go:** With eDiscovery Academy, access short, informative training videos on crucial eDiscovery concepts.

Whether you're crafting legal holds, ESI protocols, or FRE 502(d) orders, eDiscovery Assistant is your ediscovery GPS. We guide you through every step, ensuring you leverage the full potential of ESI for optimal client outcomes.

Ready to see the difference? [Contact us for a demo](#) 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/)