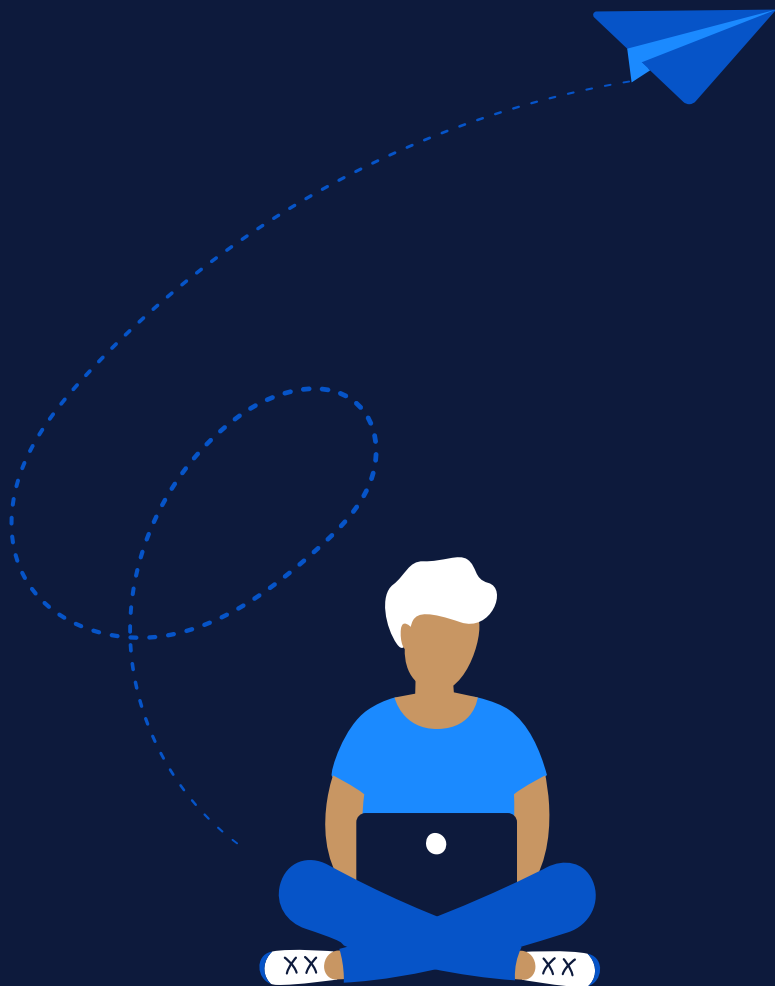




Responding to The Rise of Collaboration Apps and Remote Work: **An eDiscovery and Litigation Guide**



Electronically Stored Information as Evidence

The landmark case of Zubulake v. UBS Warburg, heard between 2003 and 2005, often marks the official beginning of legal holds for electronically stored information (ESI). A year later, in 2006, amendments to the Federal Rules of Civil Procedure (FRCP) codified the discovery of electronic documents. But at that time, email made up the majority of ESI. Needless to say, a lot has changed since then.



The Rise of Collaboration Apps and Remote Work

Even before the COVID-19 Pandemic in 2020, collaboration application (e.g. Slack) usage was rising for internal enterprise communications. According to one [study](#), the market share increased from around seven billion U.S. dollars in 2015 to nearly 16 billion in 2020.

7 BILLION
U.S. DOLLARS
IN 2015

TO NEARLY
16 BILLION
IN 2020

Since the pandemic, collaboration application usage has skyrocketed. Another study found that usage of nearly all collaboration tools increased substantially between 17 February and 20 December 2020, with Microsoft Teams growing by 3,891%, video conferencing app Zoom showing 1,788% growth, and messaging app Slack increasing by 1,073%.

MICROSOFT
TEAMS GREW BY
3,891%

ZOOM
GREW BY
1,788%

MESSAGING APP
SLACK GREW BY
1,073%

BETWEEN 17 FEBRUARY AND 20 DECEMBER 2020

Even with a return to more normal day-to-day life, the remote workplace is here to stay. One [report](#) predicts that 36.2 million workers (22% of Americans) will be working remotely by 2025. This jump in remote work is an 87% increase from pre-pandemic levels.

36.2M
WORKERS WILL
BE WORKING
REMOTELY BY 2025

87%
INCREASE FROM
PRE-PANDEMIC
LEVELS

Is Slack Data Discoverable?

The 2006 Amendment to Rule 34 of the FRCP makes the answer to this question very clear. **It states:**



Rule 34(a) is amended to confirm that discovery of electronically stored information stands on equal footing with discovery of paper documents. The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined. At the same time, a Rule 34 request for production of “documents” should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and “documents.”

There is no question whether collaboration application data from Slack, or any other application, could be potentially discoverable from this definition. More importantly, the data from these applications must also fall under FRCP Rule 26’s Relevance and Proportionality guidelines when requested during litigation.

FRCP Rule 26(b) states, “Parties may obtain discovery regarding any nonprivileged matter relevant to any party’s claim or defense and proportional to the needs of the case.”

The Rules then provide six considerations for determining proportionality:

- The importance of the issues at stake in the action
- The amount of information in controversy
- The parties’ relative access to relevant information
- The parties’ resources
- The importance of the discovery in resolving the issues
- Whether the burden or expense of the proposed discovery outweighs its likely benefit

Recent Case Law Regarding Slack Data

The FRCP sets the standards, but it's how judges interpret them that really gives organizations an idea of how the law will have a real-world impact. That's why it's important to keep up with case law to see how the courts are ruling on ediscovery-related issues.

The following cases, only two years apart, show how much can change in a short period.

Milbeck v. Truecar, Inc. (2019)

In this case, from 2019, the Plaintiffs requested Defendant's Slack data during discovery. And while the defendant was able to preserve the requested data, there was no way to "isolate any specific information, such as particular channels or users and limit the collection to only that data." Because of the relative newness of the data source, the court ruling states, "conversion and processing of the Slack data – which is necessary before any information can be extracted or any particular channel identified – will likely take at least six weeks and perhaps up to eight weeks.

“

According to the Defendants' eDiscovery provider, which has experience with Slack data, manual review will be necessary to identify the start and end of relevant conversations. Even assuming review for production could be completed in another four to six weeks after conversion and processing, the data would be available for production roughly at or close to the time of trial.

”



Because of this, the judge ruled that producing the Slack data wasn't proportional to the needs of the case and denied Plaintiff's motion to compel.

Benebone v. Pet Qwerks (2021)

In this case, from 2021, Slack data is once again requested. As it states in the ruling, “Because Benebone uses Slack as part of its internal business communications, there is no real dispute that Benebone’s Slack messages are likely to contain relevant information. The crucial issue is whether requiring Benebone to search for and produce responsive Slack messages would be unduly burdensome and disproportional to the needs of this case.”

However, by this time, “third-party tools have been developed over the past several years for collecting and reviewing Slack messages and that review and production of Slack messages has become comparable to email document production through use of these tools.”

The expert witness goes on to testify that with these tools, “Searches likely could be limited to certain Slack channels, users, or custodians – which could significantly reduce the volume of Slack messages requiring review.”



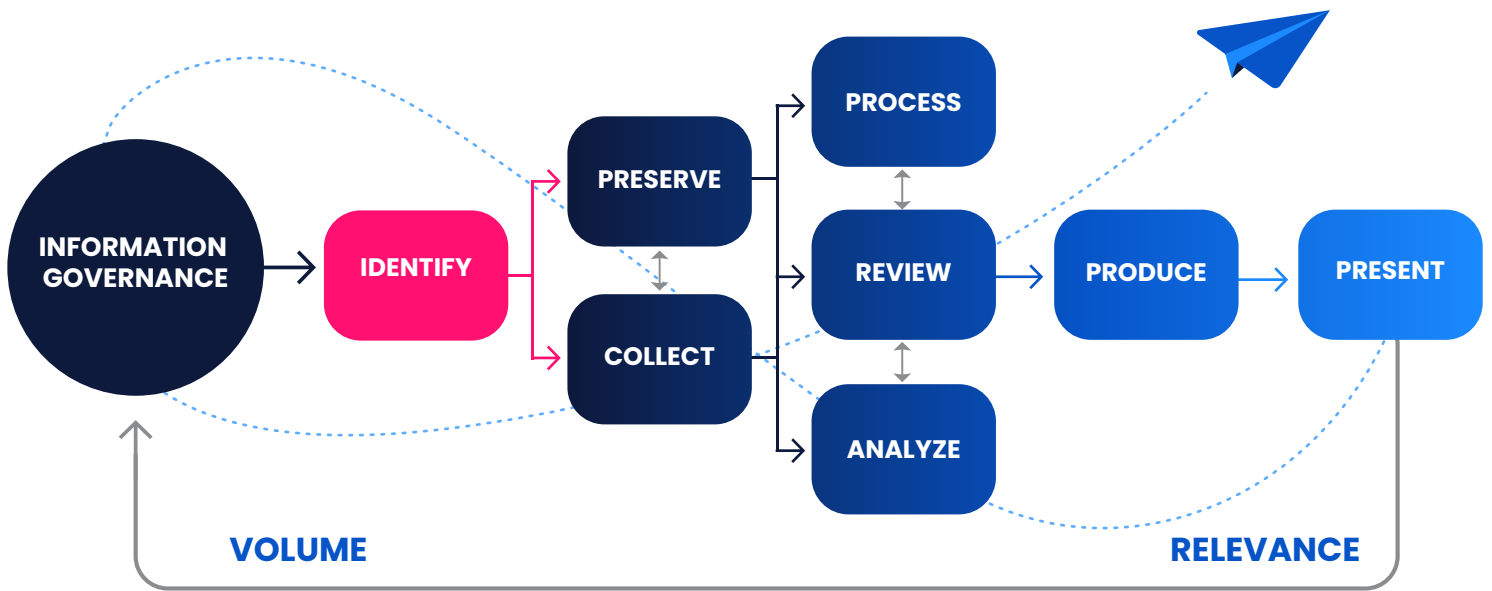
“

As such, the judge ruled as follows: “Based on the evidence presented in the parties’ briefing and at the hearing, the Court finds that requiring review and production of Slack messages by Benebone is generally comparable to requiring search and production of emails and is not unduly burdensome or disproportional to the needs of this case – if the requests and searches are appropriately limited and focused.

”

The ediscovery Process for Collaboration Data

Standards, Guidelines, and Practical Resources for Legal Professionals and Ediscovery Practitioners



The Ediscovery Reference Model (EDRM) has been a long-established visualization of the ediscovery process once litigation is anticipated.

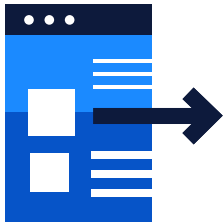
At that point, potential data custodians are identified, and a **legal hold** notice is sent, most often by an organization's in-house legal team, letting custodians know not to destroy ESI.

Usually, an organization's IT department will take the lead in **preserving the data**, especially with today's cloud-based SaaS platforms and communications channels. However, with new ediscovery tools, data can now be **preserved-in-place (PIP)**, meaning it is locked down at its source to prevent anyone from deleting or spoliating relevant data.

Organizations can **collect** the data and use **Early Case Assessment (ECA)** tools such as advanced search, analytics, and artificial intelligence to analyze the dataset. This process allows legal teams to gain early insights into the matter's case evidence and cull irrelevant data.

At this point in the process, in-house legal teams usually send the collected and culled data, exported into a usable format such as a PDF file, to outside counsel for **processing and review**. All documents included in discovery are **produced** according to the Department of Justice guidelines.

Because these final stages are often the most time-consuming and costly of the ediscovery process, in-house legal teams can reduce time, cost, and risk by only sending relevant ESI to outside counsel.



Export Formats and How they Affect the Ediscovery Process

JSON

For nearly all SaaS platforms and collaboration applications, the most common native export format is JSON. JSON uses human-readable text to store and transmit data objects consisting of attribute-value pairs and arrays (or other serializable values). And while all of the required data is preserved in this format, it's not the most usable when reviewing for potential relevance in an investigation, especially for platforms with complex user interfaces or communications channels.

When you think about how we take in the information on a webpage or application, it's not linear but dynamic. Instead of reading lines of text from the top down, a user simultaneously takes in a combination of text, images, figures, graphs, emoji, attachments, and more. A JSON export loses the visually dynamic nature of SaaS platforms.

API

Many SaaS platforms have developed application programming interfaces (API) that create a connection between their native format and other software. The purpose of APIs is to share information that may be useful to an outside program while keeping internal details of its system hidden. APIs may be custom-built for a specific pair of systems or created to allow for interoperability.

While APIs give users the ability to use 3rd party solutions to preserve, collect, and even cull data housed in a SaaS application, it's still limited to what the API is built to communicate. It still may lack some of the visual and dynamic features of the original interface.

Crawling and Scraping

Crawling and scraping tools combine to preserve website and application data as it appears live. Crawlers capture all of the pages from a single domain, and then scrapers extract predefined data fields from those pages.

For ediscovery, this technology should store data in a forensically-sound, unalterable way that provides a complete audit trail – including the hash value for the collection in the metadata – demonstrating a defensible process.

But the real benefit comes from reviewing and interacting with the dynamic web archive, which gives full context to the data and offers investigators insights that might not be available in a JSON export or even through an API. When you couple this with advanced search and data visualization tools, this technology provides a strong solution for managing SaaS application and collaboration data for ediscovery.



Litigation Challenges For Slack Data

Context is Crucial

One of the biggest challenges when preserving and collecting collaboration data, such as Slack, for ediscovery is viewing and searching that data in context. Unlike traditional email, capturing the unstructured, ongoing, and multifaceted elements of collaboration data (and related metadata) presents a significant challenge for corporate legal teams. No subject lines, no dates, no threads + emoji, gifs, attachments, share drives = ediscovery Nightmare.

This complexity is why it's essential to be able to view Slack data as it appears within the ongoing conversation. Yes, the raw data can be preserved and exported, but it is all but useless to legal teams in that form. Presentation is everything.

Emoji Are Here to Stay

Once you have the context problem solved, you have to deal with the issue of emoji, which can change the tone of the message text or carry a different meaning altogether than what they literally represent (e.g., the eggplant and the peach).

To add to the emoji challenge is the sheer number of them to keep up with. According to a [2019 article](#) in the Wall Street Journal, Slack contained 26 million emoji (at that time), with one enterprise Slack client creating more than 50,000 custom emoji in their system. Needless to say, this could pose quite a challenge should this data be needed during litigation.

Managing Legal Holds, Preservation, and Early Case Assessment on Dynamic Data Sources

Today's collaboration and SaaS data is dynamic and constantly changing from minute to minute, so it can be challenging to manage holds and preserve this type of data with traditional ediscovery methods. Because of the complexity, many organizations would have to rely on 3rd party Legal Service Providers (LSP) to collect the data, process it into a usable form, and apply ECA tools for search and culling. With this "collect everything" approach, increases in time and costs can be significant.

The Need for Speed

[FRCP Rule 26\(f\)](#) sets forth a timeline for parties to "discuss any issues about preserving discoverable information; and develop a proposed discovery plan," giving legal teams only 69 days from the initial complaint to begin framing their litigation strategy.

This rule dictates that in just a little over two months, legal teams need to identify, hold, and preserve collaboration data while viewing it within a helpful context to start building their case in time for the "meet and confer" conference with opposing counsel. They will also need to begin culling irrelevant ESI to avoid unnecessary cost and risk by sending unnecessary data to outside counsel for review.

Added Stakeholders Mean Added Data Risk

Ediscovery traditionally includes data handoffs between multiple stakeholders – IT, Outside Counsel, and Legal Service Providers – which increases risk and cost. Quickly identifying and preserving relevant data in-house without additional handoffs improves the process. It prevents overcollection and data duplication without sacrificing defensibility.

Ediscovery Checklist for Slack and other Collaboration Data

Find an ediscovery solution that:



Defensibly preserves, collects, and delivers immediate views into hard-to-capture data sources like Slack, Google Workspace, Jira, other SaaS platforms, and internal systems, while maintaining the context of the conversation, including attachments, emoji, and metadata.



Targets collections so that internal teams can quickly gain insight into communications without complication, leading to speedy resolutions while reducing risk and cost.



Gives optimal presentation of ESI, with the ability to view and interact with collaboration data as if you were looking at the live site, providing a clear understanding of the situation for a fair and quick resolution while elevating the standard of evidence during an investigation or ediscovery.



Empowers legal teams and non-technical staff with a simple and intuitive interface, so they can easily query data and orchestrate legal holds across multiple platforms – like Google and Slack – with just a few clicks.



Avoids duplicative data preservation and collection processes with PIP at the point of creation, so legal teams can collect only the ESI which is relevant to the case while automatically synchronizing across platforms, so there's never a need to re-pull or deduplicate data.



Keeps as much of the discovery process in-house to mitigate data risk, reduce cost, and meet strict deadlines.

**To learn more about
Hanzo's Litigation and
Ediscovery Solutions,
visit us at www.hanzo.co.**