



BLOG COLLECTION

Slack eDiscovery Essentials Collection



TABLE OF CONTENTS

▶ Introduction	3
▶ Overcoming ediscovery and compliance challenges: How to Defensibly Collect and Preserve Enterprise Slack Data	4
▶ Narrowing the Scope of Slack Collections: Stop Trying to Drink From a Firehose	12
▶ Don't Slack on Slack: The Challenge of Unstructured Collaboration Data in Enterprise Ediscovery	18
▶ 5 Reasons You Need an eDiscovery Playbook for Managing Your Enterprise Slack Data	25
▶ Stop Playing Tug-of-War With Your Enterprise Slack Data: Balancing the Needs of Information Governance and Ediscovery	33
▶ How to Master Slack eDiscovery & Information Governance in 3 easy steps	40



INTRODUCTION

Collaboration apps like Slack have completely changed modern-day corporate communications. Since it was launched in 2013, Slack's growth has skyrocketed. Forward-thinking companies like Intuit, Lyft, IBM, Target, Splunk, NASA, Fox, BBC, HubSpot and more are using Slack to bring productivity to their everyday work.

Slack empowers productivity through making it easier for companies to foster transparency, more frequent communication, and more clarity around individual responsibilities, team goals, and corporate strategies. The platform supports an entirely new way of communicating that is reminiscent of social media—providing a smarter and more culturally relevant communication. The control of communication is better than email, enabling people to follow channels that are specifically relevant and share information with an entire team with ease. Additionally, teams can leverage quick tools like emojis that provide an easy mechanism for a quick response to acknowledge the message or even give approval. It also helps infuse messages with personality and can add clarity of meaning. As they say, "A picture is worth a thousand words."

Nonetheless, Slack was built for collaboration not to meet the requirements of information governance, compliance and eDiscovery. You're about to read, Hanzo's Slack eDiscovery Essentials Collection which is comprised of a series of articles that delve into the collaboration platform Slack, how it's being used, the challenges it poses corporate legal, information governance, and compliance teams, and offers practical suggestions to collect, preserve and manage Slack data to mitigate risk.

We hope you'll find interesting information in these articles as you embark on learning about how you can spearhead Slack data management for your organization.

Overcoming Ediscovery and Compliance Challenges:

HOW TO DEFENSIBLY COLLECT AND PRESERVE ENTERPRISE SLACK DATA



OVERCOMING EDISCOVERY AND COMPLIANCE CHALLENGES: HOW TO DEFENSIBLY COLLECT AND PRESERVE ENTERPRISE SLACK DATA



SLACK IS THE NEW EMAIL

Slack has become a massively-important workplace collaboration tool that millions are using. We complained about email for years. Slack has answered that complaint and has successfully lured many people off of email with its intuitive design, designated communications channels, and very strong integrations that help facilitate collaboration and targeted conversations. As a result, organizations of all sizes navigated to it and Slack became a \$1B company in less than two years, which is unheard of in most cases — but that also created a problem.

WHAT'S THE PROBLEM?

If so much of a company's internal data that needs to be recorded for [compliance](#) or for [eDiscovery](#) purposes is on Slack, then, your organization needs a well-thought-out plan to collect and preserve that data, the same way organizations do with email or other repositories of electronically stored information (ESI). Slack, however, as with many new collaboration applications, is challenging to collect and preserve. The main use case of the application is, after all, communication and collaboration. Maturity in extracting data in a user-friendly format is often not at the forefront of the development roadmap. This means organizations need a plan for managing the data and also solutions to defensibly collect and preserve their Slack data.

Learn more about the challenges Slack poses for ediscovery and how to overcome them in this [on-demand webinar](#) we presented in tandem with approved.





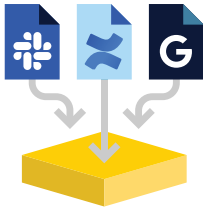
GUT REACTION: OK, OUR ORGANIZATION JUST WON'T USE SLACK!

Not so fast! While organizations often try to avoid a Slack rabbit hole by dictating “no critical business communications shall occur in Slack,” this is usually a losing proposition. Sorry to break this to you, but people are going to go with the flow. If they’re already working in Slack, they may share something business-critical in there, even if it’s not approved. If we’re being realistic, exactly how often does a corporate edict to over 1,000 people truly work?

You simply can’t dictate/policy your way out of Slack. Full stop. You will lose. So... back to that plan we were referring to previously. Time to start mapping things out. Take heart though, you’re not alone. It’s not uncommon for organizations to not have a mature playbook to refer to when they need to work with Slack data for ediscovery and compliance.

COMMON SLACK EDISCOVERY AND COMPLIANCE CHALLENGES

The ease in sharing docs, links, videos and discussing them amongst the various channels and groups, entices people to use Slack a lot. As a result, Slack produces massive quantities of data. Collecting Slack is a little like being asked to collect the ocean at large enterprises. Narrowing down what to collect becomes critical. Additionally, Slack is not a single document with attachments together, it’s a dynamic non-static form of information. Re-creating and expanding the comments and connecting to the links to outside content continues to be a formidable challenge when dealing with Slack for ediscovery and compliance. Additionally, just as with social media, the ability to delete or modify posted content can also create serious problems for organizations trying to preserve evidence.



INCLUDE SLACK AS AN OFFICIAL DATA SOURCE FOR COMPLIANCE AND EDISCOVERY

Due to relative newness, it's not uncommon for organizations to overlook Slack in traditional preservation processes. This, however, could cause you to miss out on a treasure trove of discoverable data. Ensure that your legal, risk, compliance, IT, HR and marketing departments fully understand the tool, where the data resides, and how to get the data out, should it be needed for compliance or ediscovery processes.


Ensure that you have Slack Enterprise Grid which will give you the best options for extracting Slack data. Include Slack as an official data source, establish clear usage policies, and make sure that employees know what they are and acknowledge that they will abide by them. Just as your legal hold notifications include emails, documents and other file shares, Slack now needs to be added as a data source, and included in the custodian questionnaire within the legal hold process.

HOW TO NARROW YOUR FOCUS ON SLACK DATA SO YOU KNOW WHAT TO COLLECT

But how do you identify relevant Slack data? Including Slack as a data source in your legal hold custodian questionnaires can help. There are channels, groups, and direct messages. Custodian responses can shine a light on where to look and help you understand where your custodians are having conversations, whether it be in channels or direct messages.

HOW TO COLLECT FROM SLACK

We've heard this frustration from customers. To quote the Simpsons, Ralph Wiggum, it's "unpossible," when referring to collecting from Slack. Of course, it's not impossible, but it's wise to get knowledgeable help.



DO YOU WONDER IF YOU'RE GETTING IT RIGHT WHEN IT COMES TO SLACK EDISCOVERY?

Download this free guide to get 20-pages of tips, tricks, best practices, and the common pitfalls that will help you get control of your slack data.

GET THE GUIDE

Use and Understand Slack Enterprise Grid

Slack Enterprise Grid is the top subscriber tier of Slack. Most large organizations use this.

The first tier of Enterprise is "Teams," i.e. Sales, Marketing, Operations, etc. Within your subscriber account, then, understand there are multiple teams to pull data from.

Within teams, there are:

- Channels
- Groups
- Direct Messages
- Files
- Users

All five can be treated a bit differently.

1. Channels are public channels—users can go in, read, contribute, etc.
2. Groups are channels but restricted in terms of who can join (generally they need to be invited). A group is akin to a private channel.
3. Direct messages are channels as well, but also private. It can range from just yourself to many, many people.
4. Files are downloads, documents, screen captures, etc.
5. Users are the sum total of users within your account.

It can be challenging to put all these pieces together and gain visibility around what type of business records are being created or stored. This can mean you need to take inventory to help understand the framework of the Slack data you have within your organization.



Do an Inventory Crawl

An inventory crawl goes through the Slack API at the Enterprise level and breaks down all the factors mentioned above—what teams do you have? What channels? Who is a part of direct messages?

When you combine inventory crawls with legal hold notices and custodian questionnaires, you have a good start of what to filter for and what to collect.

Taking an inventory of your Slack also helps you identify additional possible custodians and channels of interest.



Context is Critical

Once you identify relevant data, you need “the whole story” around the subject. Slack is unique in terms of how people are communicating there, so the context behind the conversations is crucial from a legally-defensible standpoint.

Slack itself offers a download for compliance purposes, but it comes in a JSON file. If you have programmers on your team with a lot of free time (HA!), you can figure that out — but most organizations don’t have those resources readily available—making the quest for context difficult, if not “impossible”.

You need a solution that takes the JSON data export and puts it into a native-like format that looks as similar as possible to the native Slack UI. This makes review much easier. The native-like rendering enables legal and compliance teams to import the information into their normal review process to glean insights from the contextual messages and quickly connect the dots.

Filter The Data You Capture

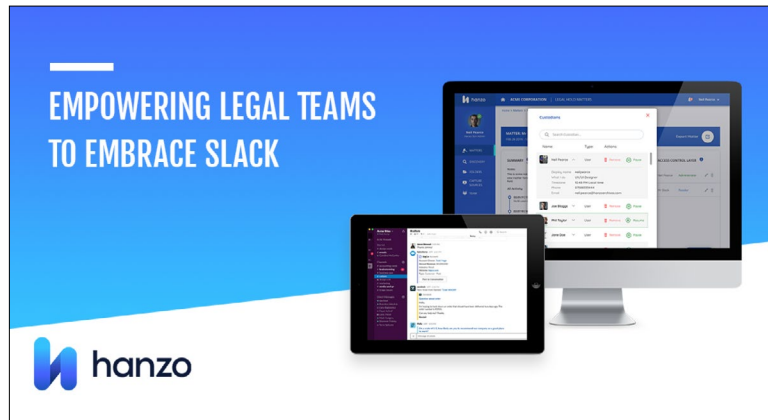
Filter by:

- Users
- Dates
- Specific channels
- Documents

There’s typically too much data in a given Slack Enterprise Grid instance to possibly analyze all of it, so you want to get the best insights you can about the data via a well-planned and well-executed legal hold process and a thorough inventory crawl to help your team target direct messages between key individuals, and identify responsive records. Remember also, that getting a natively-formatted contextual rendering of the information helps your team capture all of the information. The rendering shows the expanded view including links and their destination content—delivering the most complete data that can help speed review and enable you to use your normal review and data analysis tools.

HAVE QUESTIONS?

We know you do! It's OK! Click to learn more about Hanzo's fresh approach to Slack ediscovery.



We know [preserving and collecting Slack](#) isn't easy, but we make it easier for enterprises.

Narrowing the Scope of Slack Collections:

STOP TRYING TO DRINK FROM A FIREHOSE



NARROWING THE SCOPE OF SLACK COLLECTIONS: STOP TRYING TO DRINK FROM A FIREHOSE

There's too much data coming in and too much of it is entirely irrelevant. Plus, it can be harder than you'd expect to siphon off the trivial side conversations so that you can focus on the important ones.

If data volume were the only challenge to Slack collections, it would be manageable. Of course, it isn't; there are a few additional wrinkles.

For one thing, Slack messages tend to be short and individually incomplete, pinging back and forth in a staccato rhythm as busy employees speak in a conversational shorthand. Any single message standing alone is likely meaningless. That means that you can't capture just the individual messages—you need to collect them in their original dynamic context. (This is part of what makes separating the wheat from the chaff so difficult; they're almost inextricably intertwined).

Additionally, Slack's popularity boomed in part because of its integrations with other applications and its ability to incorporate non-Slack content. Users may upload files, share images, or link to online content. Your capture methodology must include not only the messages themselves but also any linked or associated content regardless of what app (or website) it's from.

Add all that together, and Slack collections can feel altogether ["unpossible"](#).



**PRESERVING AND COLLECTING
ENTERPRISE DATA ON SLACK:
THE GUIDE TO DOING IT RIGHT**

Managing ediscovery and compliance needs
within the hottest collaboration platform

[DOWNLOAD THE E-BOOK](#)

hanzo

TRANSFORMING THE FIREHOSE TO A MANAGEABLE STREAM

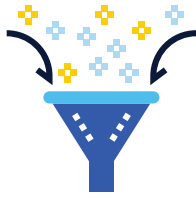
Fortunately, there are ways to limit the flood of Slack data and make reasonable collections possible. Here are three best practices to get you started.



1. Create clear policies for Slack use, backed by useful channel and group designations.

One of the challenges with collecting Slack is its casualness. Instant messaging encourages abbreviations—which aren’t always consistent—and rapid typing can lead to misspellings or mistakes. These can make searches for key terms hit-or-miss. While your collection and review tools should enable you to filter and search Slack text in a sophisticated way (see below), you can start things off on the right foot by crafting clear policies for Slack use. For example, you might limit the use of unusual abbreviations or establish rules for adding tags to work-related conversations. There’s a nifty side effect to having a policy about Slack communications: it reminds employees that their Slack conversations could be monitored or searched, encouraging them to keep it on-point and professional. (Good luck with preventing typos, though.)

Additionally, consider generating [channel](#) and [group](#) designations that will pre-sort relevant information. If everyone on the Morris project is in the @Morris group and all discussions about that project occur within the group, then any collections for litigation related to Morris should (ideally) be easy to locate.



2. Incorporate Slack into your ediscovery preservation and collection pipeline.

In many workplaces, employees initially started using Slack on the sly, without running it through their official IT pipeline. Even after the enterprise officially adopted and sanctioned the use of Slack, its “below the radar” vibe may persist. This can translate to a gap in the legal hold or broader ediscovery pipeline.

If this has happened in your organization, go back to the beginning and start over. First, make sure that everyone understands that Slack messages are potentially discoverable and subject to legal holds. You can also introduce your new Slack use policies at these meetings.

Revisit your legal hold notification process and make sure that Slack data is included in your hold notice. Incorporate Slack into both your initial custodian questionnaires and your custodian interviews to be sure you’re gathering information about what Slack messages may be discoverable. Spend some time inventorying your Slack environment and really familiarizing yourself with the different data streams within your enterprise. Your questionnaire and especially your interviews should drill down to find out which channels, groups, direct messages, tags, names, abbreviations, and words your employees are using to discuss relevant issues.



3. Use tools that enable sophisticated searching and filtering of exported data.

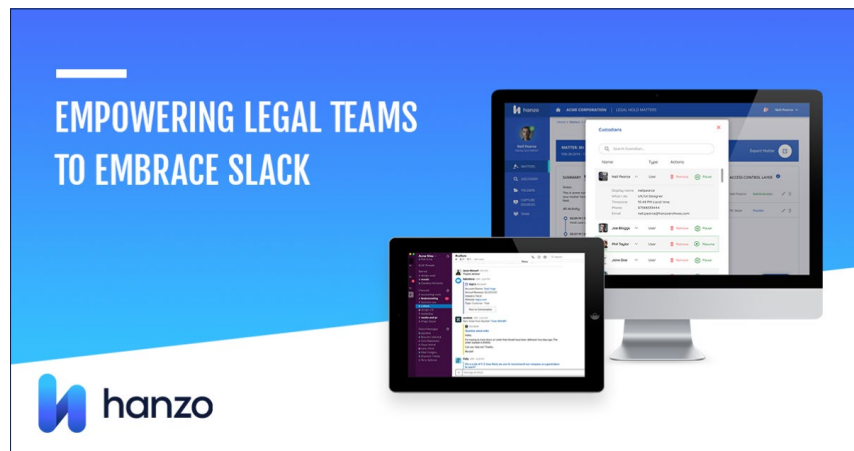
Remember that the end goal of any ediscovery effort isn't merely to find the most relevant and persuasive ESI, but to actually do something with it. In other words, you need to be able to extract potentially important data into a usable form. "Usable," for our purposes, means that you can view that information in a fully functional format, clicking on links and accessing associated files or other content. You also need to be able to search and filter your exported data so that you can continue to separate the wheat—the really good stuff you're after—from the chaff surrounding it.

Don't forget, too, that you're going to have to produce discoverable ESI to your litigation opponent and perhaps, ultimately, present it as evidence in court. If your capture tools don't allow that, you're merely gathering background information, not generating courtroom-ready content. [Slack Enterprise Grid](#) enables users to extract data from any Slack channel for compliance or ediscovery purposes using its API (application program interface). Bear in mind, though, that that exported data won't necessarily be compatible with your ediscovery review platform.

Still feel like you're going to drown in the flood of Slack data? Don't panic! Hanzo specializes in locating and capturing dynamic, complex, unstructured data from the web and from apps like Slack. We work extensively with ediscovery and compliance professionals and our capture methods are fully authenticated for use in court. Our sophisticated search capabilities and tools can tackle the most overwhelming ediscovery challenges, allowing you to navigate collected data in its as if it were live.

QUICK CHECKLIST FOR MANAGING SLACK DATA

- ☐ Understand the workspaces and channels in your organization. You can't manage what you don't know about
- ☐ What capabilities are available with each plan
- ☐ Know the Slack user roles and how they interact in the ecosystem
- ☐ Understand Slack's Structure (Organization (Enterprise Grid), Teams (aka Workspaces), Channels
- ☐ Determine edit and deletion parameters
- ☐ Set message retention and deletion rules within Slack
- ☐ Educate employees about Slack use
- ☐ Include Slack as a data source for eDiscovery and apply standard legal hold processes to Slack data just as you would for email



We'd love to show you how [Hanzo can help you master your Slack data](#), transforming the firehose into a manageable stream of useful information. [Please get in touch](#) if you're ready to hear more!

Don't Slack on Slack:

THE CHALLENGE OF UNSTRUCTURED COLLABORATION
DATA IN ENTERPRISE EDISCOVERY



DON'T SLACK ON SLACK: THE CHALLENGE OF UNSTRUCTURED COLLABORATION DATA IN ENTERPRISE EDISCOVERY

Every time we turn around, more people are using the collaboration platform Slack. As of January 2019, [Slack announced that it had surpassed 10 million daily active users](#), including 65 companies in the Fortune 100. While the free version is still the most popular, more than 85,000 individuals and organizations pay to use upgraded versions. And these daily users aren't just using Slack a little: surveys have shown that users have Slack open for [more than 10 hours each weekday](#). The upshot is that work communications that used to happen on email now increasingly happen on Slack.



This is great news for communication and collaboration—the reasons Slack was created in the first place—but less-great news for ediscovery and legal compliance. If conversations about work are now on Slack, how are organizations capturing, preserving, and producing those messages for use in litigation?

The answer, for many, is that they're not. That's partly because Slack's growth rate has been faster than most companies can keep up with, but it's also due to some serious challenges with managing the unstructured data in Slack for use in ediscovery. Those challenges range from the existential—issues wrought by the very nature of Slack—to the technical. As with most problems, the first step to solving them is understanding them, so let's take a closer look.



EXISTENTIAL CHALLENGES: SLACK'S DESIGN DEFIES TRADITIONAL EDISCOVERY

Before we even address the issues created by Slack's design, there's one small preliminary problem. To try to do ediscovery with Slack, you have to know (or at least suspect) that your organization is using it. Otherwise, you'll never go looking for it, and your ediscovery will be entirely Slack-deficient. While your policies might prohibit downloading or using apps without approval from IT, we're sorry to tell you that people don't always—gasp!—comply perfectly with company policies. There are no barriers to starting Slack use: the free version is readily available and can be downloaded and set up in just moments. Don't assume that no one is using Slack at your organization without at least investigating.

If you do find that you're using Slack, remember that it was never designed as an ediscovery tool (if it had been, we're betting its growth would have been somewhat more modest). Its *raison d'être* is improved and expedited communication and the collaboration it allows. But, no matter how good Slack may be at its intended purpose, that doesn't make it exempt from the constraints of standard business, including responsible information governance and legal compliance. In short, if anyone in your organization is using Slack for work (and it takes at least two to tango), you need to evaluate those messages for discoverable information just as you would evaluate emails, text messages, and other forms of business communication, and you need to preserve potentially discoverable information.

Herein lie the two biggest ediscovery challenges within Slack: determining custodians and defining the scope of a hold or a search.

With emails or text messages, it's easy to establish who's a custodian for what message. If you sent it or received it, voila, you're a custodian, and your entire email account can be placed on a legal hold. Then, once you've defined the scope of a discovery search—perhaps with custodians, date limits, and a few keywords—you can search through that custodian's messages for potentially responsive information.



But Slack is not an email inbox. It is, in effect, an unstructured digital bulletin board or a ticker tape. Within a given channel or message history, Slack messages unfold chronologically, without any indication of who's read (or even scrolled past) what messages. A “custodian” for a Slack message, then, could be anyone who belongs to the channel in which that message appears—meaning you have to place a legal hold on the entire channel.

When it comes to defining scope more granularly, the chronological nature of Slack feeds presents another problem: conversations unfold slowly, over the space of many messages, often interrupted by irrelevant messages. Instead of self-contained emails that present a single conversation in a somewhat-organized fashion, unstructured Slack conversations need to be read in their full context—often spanning multiple screens—to be truly understood. That means you can't just preserve or produce those individual messages that contain keywords; you need to also capture everything around them so that they make sense.

Okay, so you have to determine whether you're using Slack, rethink your definition of custodians, and expand the way you scope discovery. Then you're good to go, right? Sorry, still no.

TECHNICAL CHALLENGES: SLACK ISN'T AN EDISCOVERY TOOL

Slack has recognized that organizations need a way to preserve messages, but because it's not designed for ediscovery, the tools that it's introduced are blunt instruments at best. Those tools are lacking in part because they attempt to resolve both information governance challenges (the need to defensibly delete outdated information) and ediscovery challenges (the need to preserve potentially relevant and discoverable information) in one fell swoop.

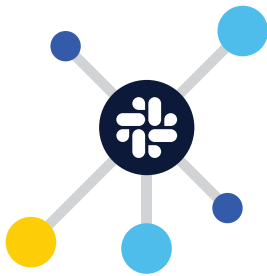
Case in point: Slack has introduced functions that allow organizations to set a message retention period, after which messages are automatically deleted. It's also added the ability to put an entire channel on legal hold, so that messages in that channel aren't deleted, preventing spoliation. (Note that if you're using the free version of Slack, you've only got access to the [most recent 10,000 messages anyway](#)—so anything older is not readily available to you.)



Slack's legal hold function, though, is entirely binary. It's either on or off, with no ability to specify particular dates. This is probably fine if you only have one litigation matter or one legal hold at a time. But if you're in a more typical organization, where you at least sometimes have overlapping legal holds for different custodians, you'll quickly find that you can't release the first hold without losing information that might be discoverable under the second. That means that once you start implementing holds, you may find that they're effectively permanent. In other words, you'll either release legal holds and potentially spoliage messages in the process, or you'll maintain those holds and thereby retain messages for much longer than you otherwise would.

There's an obvious solution here: export data that you need to save outside of Slack and continue deleting messages in Slack according to your records retention policy. Boom, you're done—right?

Yes—but exporting Slack data in a useable format is a lot harder than you'd think. Slack's only export tool uses a JSON file type, which is unwieldy at best. Each day of activity in each channel creates a separate JSON file—so if you're tracking a conversation that spans multiple days, you'll have to toggle between different files to review it or make any sense of it. And you know what you don't need in ediscovery review? Something that's going to slow the process down or make it even more expensive.



Then there's also another problem that could probably fit under either of these broad categories: the enormous use of Slack, combined with its ability to integrate with other apps and its ability to incorporate links and files of all types, means that there are simply massive amounts of complex and varied data within Slack. As with all types of ediscovery, the more data, the harder the task.

Finally, we mentioned this in passing a moment ago, but it's worth bringing up again: if you're going to use Slack at your organization, you need to ensure that you're using the right version. The free version doesn't allow any preservation of messages, so that's not an option. While the premium version allows some increased capabilities, those tools obviously fall short of what's needed for most organizations. If you have any complex litigation or ediscovery needs, your best bet is to choose Slack Enterprise Grid, which is optimized for ediscovery support.

Hold on, though—didn't we just say that Slack's ediscovery tools aren't sufficient? Why do you need Enterprise Grid if it won't provide you with a comprehensive ediscovery solution?

Because Enterprise Grid gives you access to Slack's discovery application programming interface (API), and that's what enables Slack to work with a dedicated ediscovery tool that does solve these challenges.

Like what? We're glad you asked.



HANZO HOLD OVERCOMES THE CHALLENGES OF EDISCOVERY IN SLACK

Realizing that all of these problems existed was what led us to create a solution: Hanzo Hold. It allows users to capture potentially responsive messages in a protected external repository associated with a particular hold. Each individual legal hold can be implemented and released as needed without disrupting the archives associated with other holds. And Hanzo Hold doesn't care how big your archive is or how many associated files or file types are embedded. Best of all, the archives created by Hanzo Hold can be reviewed naturally, in the order that messages were written in a channel, without shuffling between different files or trying to line up which conversation is which. That saves time—and money—in review while ensuring that you can see every part of a message's history.

Slack is revolutionizing the workplace, but it shouldn't be destroying your legal compliance in the process. Don't slack off on figuring out how to manage ediscovery of Slack messages. [Start a conversation with Hanzo](#) today and learn what it means to capture confidence.

5 Reasons You Need an eDiscovery Playbook for Managing Your Enterprise Slack Data



5 REASONS YOU NEED AN EDISCOVERY PLAYBOOK FOR MANAGING YOUR ENTERPRISE SLACK DATA

The collaboration app Slack sounds, from its full name, like it should be designed for discovery in litigation—“Slack” is actually an acronym for “Searchable Log of All Conversation and Knowledge.” Isn’t that what we’re aiming for in ediscovery?



What can we say: sometimes names can be deceiving.

While Slack is searchable, and it’s often positively packed with discoverable information, it’s not like the structured email data that ediscovery practitioners have grown accustomed to working with. While your existing ediscovery playbooks give you a written, repeatable, and defensible plan for identifying, preserving, collecting, processing, culling, reviewing, and ultimately producing discoverable data, those approaches don’t work well with Slack data.

Here are the top five reasons why you need a dedicated playbook to help you make sense of your Slack data and successfully shepherd it through every stage of ediscovery.

1) SLACK—LIKE OTHER INNOVATIVE TECHNOLOGIES—IS HERE TO STAY

You may be thinking you'll just sit this one out. After all, if Slack data is so difficult to manage, surely you could simply prohibit its use and find or wait for a different collaboration tool, right? And Slack has been posting multimillion dollar losses for the last year or so; maybe it's not worth figuring out how to manage it in ediscovery. You don't need a playbook for Slack if you don't use Slack!

But here's the thing: Slack is the direction that technology will be evolving in, whether your company evolves along with it or stagnates with familiar older technologies. Because the upcoming generation of workers places a high value on communication and collaboration, there will only be more, not less, of these instant message board apps in the future.

What's more, companies that seek to attract new talent also make themselves more attractive by demonstrating their ability to embrace innovation, which includes adopting new technologies. While you could choose to ignore innovative technologies like Slack, you're likely to find that that's a future-limiting move as technology in the workplace—and the generation manning that workplace—continues to change at a breakneck pace.



PRACTICE TIP:

Don't try to "policy your way out" of using Slack. Instead, create workable policies that ensure you know what apps your employees are using to communicate and what sorts of communications happen where.

2) SLACK DATA IS POTENTIAL EVIDENCE, WHICH MEANS IT'S DISCOVERABLE

Under Federal Rule of Civil Procedure 26(b)(1), the scope of discovery includes “any nonprivileged matter that is relevant to any party’s claim or defense and proportional to the needs of the case.” Information does not need to be admissible as evidence to be deemed discoverable.

In businesses everywhere—including 65 companies on the Fortune 100—much of the internal business communication that used to happen on email has now moved to Slack. But, as with other types of evidence, if any parts of those communications are relevant to a litigation matter, they’re still discoverable. That means you need to know about the data you have within Slack and be prepared to identify, preserve, review, and ultimately produce that data in ediscovery. Not to mention that, aside from discovery you provide to an opponent, you’re going to want to be able to analyze Slack data for your own use in litigation.



TIP

PRACTICE TIP:

Incorporate Slack—and other communication and collaboration tools—into your standard custodian questionnaires and legal hold notifications so that custodians are prompted to disclose their potentially relevant Slack communications.

3) SLACK DATA IS SUBJECT TO SPOILIATION—AND ATTENDANT SANCTIONS

This is the flip side of the discoverability coin: because Slack data is potentially discoverable, you may be obligated to preserve it from the moment that litigation becomes reasonably likely. Fail in that duty, and you could find yourself subject to sanctions for spoliation, up to and including dismissal or default judgment of a case or claim.

Several aspects of Slack raise specific spoliation concerns. First, if you're using the free version, you can only access the most recent 10,000 messages (and you'd be surprised how quickly you'll hit that limit). If you have 9,950 messages in Slack when you learn that messages 15 through 30 are subject to a legal hold, you'll need to act quickly to either stop the addition of messages or to gain unlimited message access.

Slack also has a setting that allows users to edit or delete their individual messages, opening up another avenue for potential spoliation through later manipulation of conversations. And Slack's internal ediscovery tools are blunt instruments at best, as they don't allow users to implement targeted legal holds on specific custodians. (We'll get into the trouble with custodians more in a minute.)



TIP

PRACTICE TIP:

If you allow for edits and deletes, make sure that your Slack administrator has set Slack to preserve edits and deletes.

4) SLACK DATA ISN'T ALWAYS EASY TO ACCESS

How do you get data out of Slack, anyway? While ediscovery professionals have learned how to deal with email and other established data types, it can be surprisingly difficult to get Slack data out of the app and into an ediscovery review platform.

As we mentioned above, this is especially true in the free, limited-function version of Slack. But even within paid versions, Slack's native export function uses JSON files that are hard to navigate—each day in each channel is saved in its own file—and consequently slow down review.



TIP

PRACTICE TIP:

If you're involved in more than one litigation matter at a time, you need to upgrade to Slack Enterprise Grid so you have access to Slack's discovery application programming interface (API), which gives you more options for exporting data.

5) SLACK DATA IS UNSTRUCTURED—WHICH MEANS YOU NEED A SEPARATE PROCESS FOR MANAGING IT

Most data in ediscovery is structured—organized into “bins” by custodian. Slack data is different. It doesn’t sort data into mailboxes or files by custodian. Instead, its messages primarily operate as a virtual bulletin board, posting information chronologically for anyone in a channel to see. Messages are marked read as soon as a user scrolls past them, but Slack doesn’t know who’s actually read what. This message organization dramatically redefines “custodians” for purposes of ediscovery; everyone who has access to a channel is a custodian for all of the messages in that channel.

The unstructured nature of Slack data makes it entirely unlike the ediscovery data you’ve grown accustomed to working with. Not only do you need to rethink who is a custodian, but you also have to create new rules for scoping discovery due to the chronological, rather than conversational, presentation of messages. The context for a Slack message may take several screens—interrupted and punctuated by irrelevant remarks and separate conversations—to be fully revealed. This, more than anything, illustrates why you can’t just fold Slack in to your existing ediscovery playbooks. You need a whole new approach that accounts for the unique features of Slack data.



PRACTICE TIP:

Plan on using an external preservation method to implement legal holds on Slack data. Why? First, because Slack data is not organized in a way that allows for targeted legal holds on individual custodians, so you have to preserve entire channels. Second, because Slack’s internal information governance and ediscovery tools are binary rather than granular—they either preserve all messages in a channel forever, or they delete all messages after a set period of time. In combination, this means it’s easiest to preserve messages for a legal hold outside of Slack and let Slack itself delete messages in accordance with your records retention policy.

BUILD YOUR SLACK EDISCOVERY PLAYBOOK WITH HANZO HOLD

As a company, Hanzo was formed to meet the unique needs of regulatory compliance and ediscovery professionals—and we’ve embraced new technologies like Slack. That’s why we developed Hanzo Hold, a dedicated Slack preservation tool that solves the ediscovery challenges posed by Slack’s unstructured data. If you’re ready to learn more about how to put together your Slack playbook for eDiscovery, get this 20-page free guide.

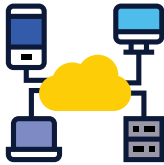


Stop Playing Tug-of-War With Your Enterprise Slack Data:

BALANCING THE NEEDS OF INFORMATION GOVERNANCE AND EDISCOVERY



STOP PLAYING TUG-OF-WAR WITH YOUR ENTERPRISE SLACK DATA: BALANCING THE NEEDS OF INFORMATION GOVERNANCE AND EDISCOVERY



If your organization is using the collaboration application Slack—joining the ranks of its [10 million daily active users, including 65 companies on the Fortune 100](#)—you might be surprised to learn just how much relevant business data is contained within its messages. From project discussions and client notes to interpersonal communications that might demonstrate a pattern of harassment (or, hopefully, not), Slack is packed with the internal chatter that used to occur primarily over email.

But how do you manage the data within Slack? What do you do with it? How long do you keep it, and how do you keep it? How do you maintain Slack messages that are potentially relevant to pending or likely litigation—and how do you access those messages for ediscovery review?

For information within Slack, as for other types of business information, you may feel like your data is the rope being yanked around in a game of tug-of-war between information governance and ediscovery.

Fortunately, there's a way to extract value from your Slack data while minimizing the risks it poses—but you have to go outside Slack to find that solution.

SLACK IS FULL OF VALUABLE—AND RISKY—BUSINESS DATA

A large portion of the conversations that the people within your organization used to have over email have likely migrated over into Slack. And, as with email and its myriad attachments, not only is there raw information contained within individual Slack messages, but Slack also seamlessly incorporates a wide range of file attachments. What's more, Slack allows integrations with a host of other apps, from document repositories like Google Drive, Microsoft OneDrive, and Box to project management tools such as Trello and Asana and even communication tools like Zoom.

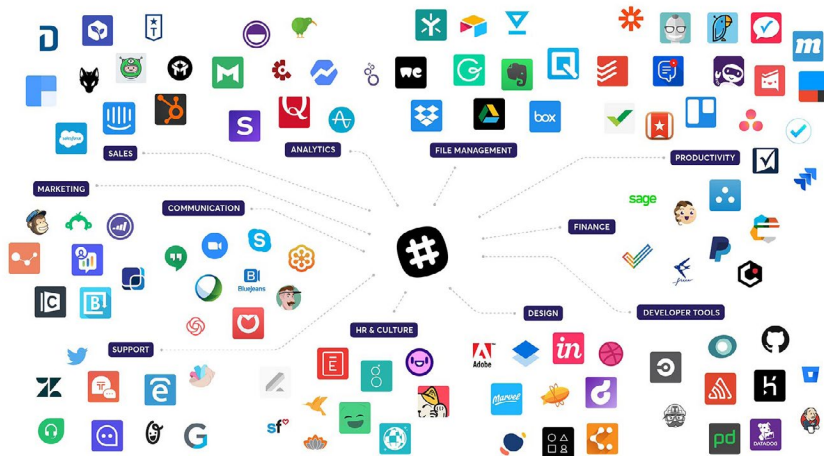


Image credit: [Slack](#)

The bottom line is that there's a plethora of data of all types hanging out in your Slack application. Some of that data has clear business value: it may show exactly how and when an intellectual property asset was developed or demonstrate an individual's knowledge about a problem or a situation that's relevant to an ongoing litigation matter. Other data—conversations about lunch, long-running jokes, or the back-and-forth negotiation of scheduling a meeting—has little or no value to the business (or, for that matter, to anyone else).



Similarly, the longevity of that value varies. Some data has an evergreen value, such as information about a study supporting the therapeutic benefits of a pharmaceutical product. Other data, such as information about an individual employee or document, has only a time-limited or short-term value.

At some point, all data—from the perpetually priceless to the irretrievably worthless—poses some level of risk. If nothing else, maintaining gigabytes and terabytes of low-value data needlessly drives up the cost of ediscovery.

This conflict between the value of data and the risks posed by that data sets up a tug-of-war between the goals of information governance, on the one hand, and ediscovery, on the other.



BALANCING THE GOALS OF INFORMATION GOVERNANCE AND EDISCOVERY CONCERNING DATA'S VALUE AND RISKS

It's an oversimplification, but the overarching goal of information governance is to get rid of data as soon as its purpose has been served and its value extracted. If ediscovery weren't acting as a counterbalance, no data would be preserved once it had been analyzed and stripped of useful business knowledge. In the view of information governance, most data imposes unacceptable burdens, including the risk of security breaches and informational leaks, the time wasted organizing and searching through excessive amounts of data, and the cost of storage.

By contrast, ediscovery professionals err on the opposite side of the spectrum, preferring to preserve practically all data for practically forever. It's true that the costs of data storage and ediscovery processing and review are indisputably linked to data volume, driving up costs for every additional gigabyte of data. But those who practice ediscovery find the risks of data loss or spoliation—and the attendant sanctions, which can range from monetary penalties to outright dismissal of a case or claim—to be higher.

To be clear, there are limits on what must be preserved in anticipation of litigation. Discovery only encompasses information related to reasonably anticipated claims, and the quantity of that information should be proportional to the value of the claims. Information that has been defensibly deleted before any trigger event occurs to initiate the duty to preserve is not subject to spoliation sanctions—though an organization may still have to defend its processes and explain when and why it deleted certain information. It's enough to make ediscovery professionals gun-shy about data deletion.

And when we're talking about Slack data, there's an added complication: Slack data, unlike email data, is unstructured, making it difficult to access, scope, or review in the context of ediscovery. That's why you need to have a dedicated playbook for managing ediscovery with enterprise Slack data.



So, how can you reap the value of the data your organization holds within Slack while effectively managing the risks of either keeping it too long or not keeping it long enough and inadvertently spoliating it? Do you pull too far to the data deletion side, getting rid of nearly everything and risking a spoliation claim, or do you keep nearly everything, driving up your data costs and especially your ediscovery review costs but minimizing the risk that you'll accidentally delete something relevant to pending litigation?

This is where it can feel like your organization is playing a game of tug-of-war between information governance and the ediscovery team or the entire legal department—and your Slack data is the rope.



A BETTER APPROACH TO MANAGING SLACK DATA

The thing is, Slack has created internal data-management tools that solved for the information governance problem. Slack now allows users to set a data retention period, after which messages are automatically deleted. This limits the risks of maintaining outdated data and manages data volumes. But that tool didn't solve for the ediscovery problem at all. Slack still doesn't support any targeted message-preservation efforts; you can either have data retention on, keeping all of your Slack messages, or you can have it off, deleting everything beyond your set time limit. To be clear, that's not even a complaint about Slack—it's been designed as a collaboration tool, not an ediscovery or information governance tool. It's a simple fact that no tool does everything—you can have a perfectly good Dremel multi-tool that's great for cutting and grinding and polishing, but that doesn't make it a good hammer.

That's why we designed a specialized technology, [Hanzo Hold](#), that allows users to implement legal holds and preserve potentially relevant data outside of Slack, in a separately maintained archive. With your discoverable data safely secured, you can set your data-retention period to whatever you choose, managing the risk of maintaining outdated information without running afoul of ediscovery obligations.

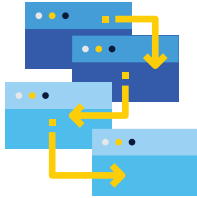
Don't ask a collaboration tool to do the job of an ediscovery tool. Stop the tug-of-war between information governance and ediscovery with Hanzo Hold.

To learn more, check out our [ebook](#) or [contact us](#).

How to Master Slack eDiscovery & Information Governance in 3 easy steps



HOW TO MASTER SLACK EDISCOVERY & INFORMATION GOVERNANCE IN 3 EASY STEPS



Slack is huge, showing a [massive growth](#) rate since its launch—and it's a huge ediscovery problem.

Why? Unlike the data within familiar ediscovery formats such as email, the data in Slack is [unstructured](#). This makes it hard to figure out who data custodians are, difficult to set limits on scope, and basically impossible to handle with traditional ediscovery tools.

To make a tough situation tougher, if you do manage to solve the ediscovery problem by retaining Slack messages for legal holds, you create an information governance problem by keeping additional data (most of it irrelevant) past its scheduled deletion date. Or, on the flip side, if you try to maintain record retention schedules and delete older data, you create not just the possibility but also the near certainty that you'll spoliage relevant data that was subject to a preservation obligation. Hello, rock, I'd like you to meet my friend, hard place.

But, as they say, just because it's hard doesn't mean it's impossible. Indeed, it's absolutely possible to manage both ediscovery and information governance with Slack data—though you might need a little help.

These three easy steps will get you started.



1) ESTABLISH DEFINITIONS AND SLACK USE POLICIES.

The first step in managing Slack data is getting clear about what Slack data you care about, which means you're going to have to think about who your custodians are and what the scope of discovery should include.

Ordinarily, you need to identify custodians for an ediscovery matter—Bob in sales, Cindy in accounting—but you don't need to define what it means to be a custodian. When you're putting a legal hold on an email account, the owner of the account is the person who sent or received those messages, thus, of course, the custodian. It seems a bit silly to even have to say it, right?

Slack is different. Aside from direct messages in Slack—which do operate essentially like email in terms of who sees them—most Slack communications occur on public or private “channels.” Slack channels are the bulletin boards of the digital world. Anyone who's a member of a channel might see any message (or, for that matter, every message) in that channel. They may never contribute to the channel, making them practically invisible, but they can still be there quietly reading. Or not; you can't tell whether someone has read a message in a Slack channel unless they've directly responded to it.

So what Slack messages belong to a particular custodian? If you're putting a legal hold on the communications from Bob in sales, what Slack messages should you include? In our view, you have to include every channel that Bob belongs to as well as his direct messages. That means you might suddenly be talking about half of your Slack data for just one custodian.

Then there's the scope of a hold. According to [Federal Rule of Civil Procedure 26\(b\)\(1\)](#), the scope of discovery encompasses "any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case." So you grab the messages that contain the keywords you've identified with opposing counsel, right?

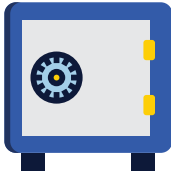
Well, no—or at least, you can't stop there. Sure, you need the messages with keywords, but most Slack communications are one-liners rather than complete thoughts. The meaning or impact of a given message might take screens of text to unfold. That means your scope can't be limited to just the messages with keywords; it must encompass all of the surrounding context.

While you're sorting out these definitions, adopt Slack use policies that will give you at least a modicum of control over what happens on Slack and where it happens. Consider including the following terms in your Slack policy:



- how different channels can be established and what type of communication each channel can be used for;
- who can be added to channels—internal team members only or external participants too?—and how people can be added;
- what information can be discussed on Slack; and
- whether users can edit or delete their own Slack messages using the app's options.

Finally, it's always a good idea to remind employees that all of their Slack messages—like their emails, work-related text messages, and work documents—may be subject to discovery. Slack feels casual and "off the record," but it's not. Before writing anything, imagine your words being read aloud to a jury; do they still sound clever and necessary? If not, it might be best to keep that thought to yourself.



2) PLAN FOR LEGAL HOLDS AND INVEST IN THE TECHNOLOGY YOU NEED TO MANAGE THEM

Once you've defined your custodians and determined how you'll scope a preservation effort for Slack data, it's time to plan your legal hold implementation. Where will you preserve Slack messages and how?

Slack has an option for legal holds, allowing users to retain data that's subject to a hold even if they've implemented a record retention schedule. (We'll return to this in step 3, below.) But there's an enormous problem with Slack's legal hold functionality: it's either on, or it's off. If you only have one legal hold, that's probably no big deal. Turn the hold function on when your trigger event occurs; turn it off when the matter has concluded.

But the moment you have multiple, overlapping legal holds, you find yourself in a permanent state of hold. You can't lift one hold to delete outdated messages without also lifting any current holds, potentially spoliating relevant discoverable data.

That's why we recommend that all legal holds be maintained outside of Slack rather than keeping all messages within the app. That requires creating a backup of the channels to which your custodians belong, perhaps limited (to some extent) by keywords or relevance filters—but having that external backup allows you to delete messages in your Slack application as they pass your record retention expiration date.

To export data outside of Slack in a meaningful, usable format, you are going to have to make some technology investments. For starters, you can't get away with the free version of Slack—which only gives you access to your [most recent 10,000 messages](#) anyway.

Instead, we recommend that you upgrade to Slack Enterprise Grid, which allows access to Slack's discovery API (application programming interface). That's what lets you export Slack data into other ediscovery tools and enables more sophisticated Slack data management.



3) PLAN FOR DEFENSIBLE DATA DELETION

Okay, you've defined your terms, implemented some Slack use policies, and figured out a way to preserve potentially discoverable Slack data outside of the app. Now there's just one step left—and fortunately, it's an easy one: establish a record retention schedule and set up your Slack data to self-destruct once it exceeds its expiration date.

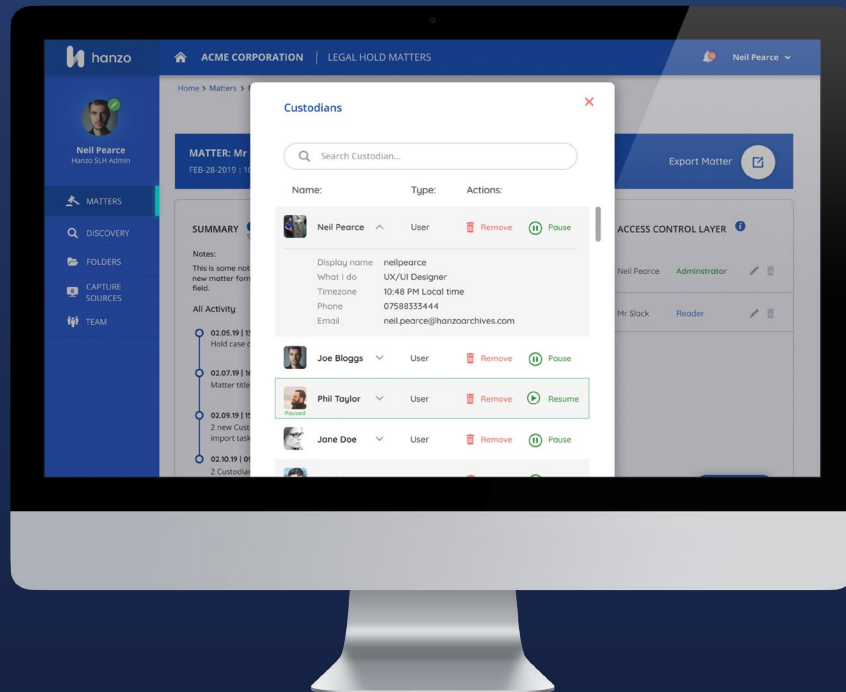
Slack has an internal function that allows you to set automatic record retention and deletion schedules. That means you can have messages deleted as soon as they exceed 30 days, 90 days, or whatever period your organization believes best balances the risk of retaining outdated data against the value of that data. And again, having your Slack data on an external legal hold gives you the option to implement this defensible data deletion option within the application itself without risking the loss of any data subject to that legal hold.

Still overwhelmed by the difficulties in managing your Slack data in accordance with your ediscovery and information governance obligations? Hanzo can help! We've designed a technology that's dedicated to preserving the unstructured and amorphous data within Slack. Hanzo Hold allows users to implement defensible legal holds, preserving potentially relevant discoverable data in a separately maintained archive outside of Slack. With your discoverable data safely sequestered, you can allow your Slack application to delete outdated information, reducing the risks of retaining extraneous data without running afoul of your ediscovery obligations.

To learn more, check out our blog on how you can create a [dedicated playbook](#) for ediscovery and our [ebook](#) that explains all there is to know about ediscovery with Slack data. Or just [contact us](#) to schedule a meeting. Slack data is manageable—and we can show you how.



PRESERVE EXACTLY THE SLACK DATA YOU NEED. NOT MORE.



Best Practice eDiscovery and Compliance for Enterprise Collaboration

Hanzo Hold empowers corporations to apply a legal hold—including silent holds—to enterprise Slack communication data, adhere to information governance policies, and meet the duty to preserve data for litigation and compliance.

REQUEST A DEMO