hanzo

SLACK COLLABORATION DATA:
The Guide to Preserving and Collecting Critical Enterprise Information

The data in Slack is essential to ediscovery and regulatory compliance. Here's how to manage it defensibly.

AUTHOR: BRAD HARRIS

INTRODUCTION TO SLACK

Slack proclaims that its collaboration platform is "where work happens."

Ever since organizations across the country and around the world have shifted to remote work to slow the spread of the coronavirus, work truly happens everywhere—which makes Slack more important than ever. Slack is where colleagues stay connected, both professionally and personally. It's where junior employees get advice and mentorship. It's where team members share updates, ask questions, and make plans.

Wherever your employees are, Slack brings them together and helps them do their work.

> **Slack is where work happens**
>
> Slack is a collaboration hub, where the right people and the right information come together, helping everyone get work done.

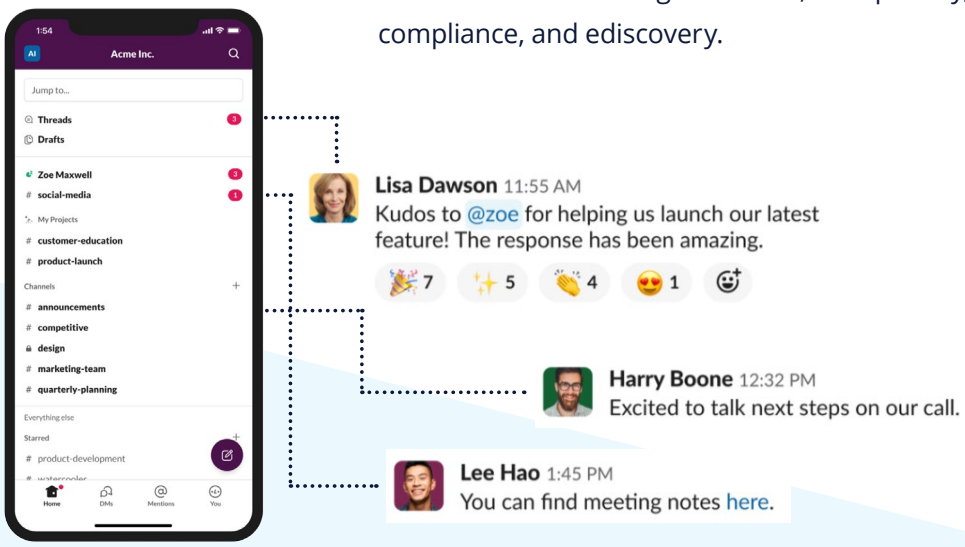
The upshot of that is that there's an absolute gold mine of enterprise data located within the Slack application. In fact, the name "Slack" is an acronym for a "Searchable Log of All Conversations and Knowledge."

If your work hinges on diligent information governance, this might make your head explode. All conversations? All knowledge? Kept around forever for anyone to see?

Mind you, we're not talking about a few hundred or even a few thousand messages here. We're talking about the volume of messages generated by more than 1 billion minutes of active use each weekday.[1]

Yikes.

It may be true that keeping organizational knowledge around—even forever—is a great idea for encouraging collaboration, building teamwork, and leveling up operations based on past learnings. But having years of conversations just lying around—the relevant and the irrelevant, the timeless and the passing fancy, the project-oriented and the social—opens up a Pandora's box of potential risks related to information governance, data privacy, confidentiality, compliance, and ediscovery.



1. *Slack Technologies, Inc. "Slack CEO Stewart Butterfield Shares Updated Business Metrics During Tweetstorm on Impact of COVID-19." Slack HQ (news details). March 26, 2020. Accessed August 17, 2020.*

Many organizations have turned a blind eye on Slack data, letting it proliferate without establishing the information governance strategies and policies necessary to establish its appropriate use. Slack may have come into the organization as an unauthorized shadow application, or it may have been adopted piecemeal without an overarching guidebook or strategy for its use. Companies often realize that they never developed playbooks or specific processes for managing Slack data, and they discover—sometimes too late—that the methods they use for email data don't work at all with Slack, due to the way it organizes and exports data.

With the pandemic-driven shift toward remote work fueled and enabled by collaboration applications like Slack, the time has come for ediscovery professionals to get serious about managing collaboration content. Data within Slack must be treated with the same care and intentionality as more traditional forms of electronically stored information (ESI)—emails, memos, corporate documents, and the like. Organizations cannot continue to kick the can down the road, deferring decisions about how to meet their discovery obligations, govern their information, mitigate the risks of that information, or comply with regulatory requirements.

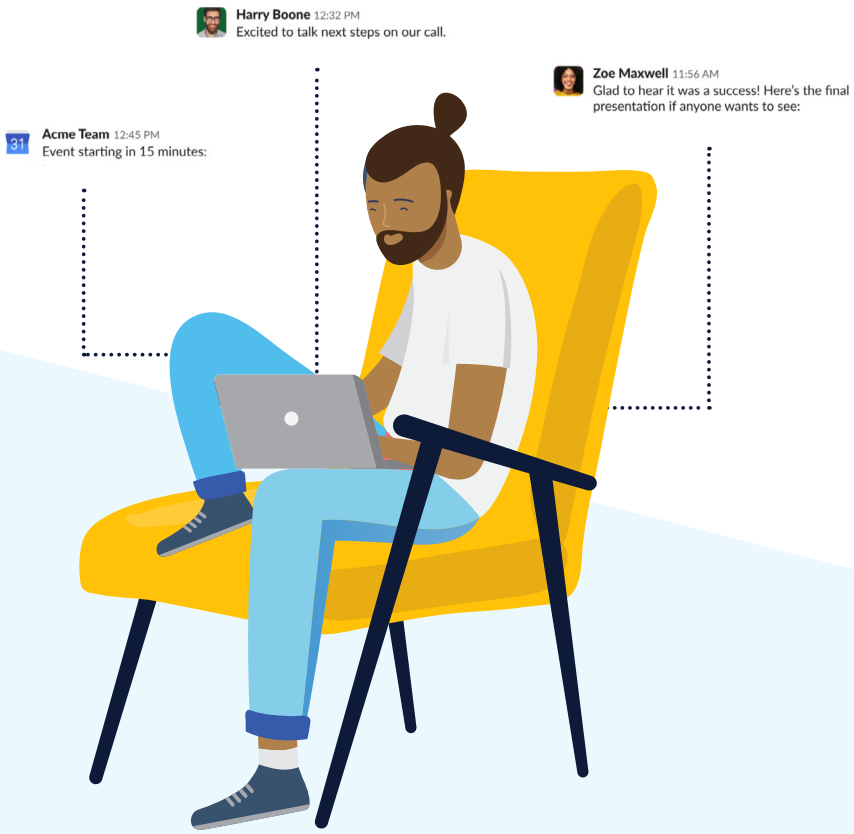
"Slack's not specifically a 'work from home' tool; it's more of a 'create organizational agility' tool. But an all-at-once transition to remote work creates a lot of demand for organizational agility."

– Slack CEO Stewart Butterfield[2]

2. Butterfield, Stewart. Twitter post. March 25, 2020, 10:23 p.m. Accessed August 17, 2020. https://twitter.com/stewart/status/1243000506605174785

We're here to help. This guide will first explain how and why organizations use Slack and set out the pitfalls that they may encounter in doing so. We'll then walk you through how to preserve and collect data for ediscovery, investigations, and regulatory compliance while maintaining a reasonable information governance and record retention schedule. The guide wraps up with a 12-step process that will walk you through how to incorporate Slack into your ediscovery and compliance frameworks.

Ready to create the comprehensive Slack playbook you need? Let's get started by looking at what Slack does and how it works.



> ...while most plans allow organizations to set data retention periods after which information is automatically deleted, that setting is either on or off; it does not allow for the preservation of specific messages that may be subject to legal holds or compliance demands.

HOW ORGANIZATIONS USE SLACK

By its own description, "Slack is a place where your team comes together to collaborate, important information can be found by the right people, and your tools pipe in information when and where you need it." Slack allows real-time interactions within groups of people, organized around projects, teams, or specific needs—which, in these pandemic times, definitely includes straight-up socializing.

There are essentially no barriers to using Slack: Users can access Slack online or through a desktop or mobile app, and they can get started immediately with the free version. Organizations can continue to use the free version or can sign up for one of several paid levels that offer additional functionality *(see next page)*.

Note that for all of these plans, the data management tools have fairly basic functionality. For example, while most plans allow organizations to set data retention periods after which information is automatically deleted, that setting is either on or off; it does not allow for the preservation of specific messages that may be subject to legal holds or compliance demands.

LEVELS AND LIMITS OF SLACK PLANS[3]

Slack comes in two basic flavors: standard Slack, designed for small to mid-sized organizations, and Slack Enterprise, for larger and more complex organizations.

Standard Slack Plans

- **FREE:** This version is very limited; it stores and allows searching of only the most recent 10,000 messages and offers only 5 GB of data storage. (You'd be surprised how quickly a team can reach 10,000 messages and 5 GB!)
- **STANDARD:** The first paid level allows an organization to retain and search its entire message history, including 10 GB of storage for each member. This level also allows for automatic deletion of messages after a specified data retention period and limited data analytics. Data exports are not enabled with this plan.
- **PLUS:** This plan adds to the standard features, doubling per-member storage, enabling some data export functions, and allowing organizations to choose their data residency, among other upgrades.[4] Data exports under the plus plan are not automated and can be unwieldy, which we'll get into more in a moment. The plus plan still only allows for a single workspace.

Slack Enterprise Grid

Designed for larger organizations and those that need to be able to deploy ediscovery and compliance features, Slack Enterprise Grid gives users access to the Slack application program interface (API), which can be used to export functional archives. Slack Enterprise Grid also allows organizations to design and operate multiple interconnected workspaces and create multi-workspace channels.

3. Getting Started: Slack Plans and Features. Accessed August 17, 2020. https://slack.com/help/articles/115003205446-Slack-plans-and-features-
4. Workspace Administration: Data Residency for Slack. Accessed August 17, 2020. https://slack.com/help/articles/360035633934-Data-residency-for-Slack

SLACK BY THE NUMBERS

Slack only launched publicly in 2014, yet it rapidly grew to a multibillion-dollar company—and the coronavirus pandemic, with its need to power remote work, has accelerated its adoption. As of September 2019, Slack had reached 12 million average daily users, with more than 6 million of those accessing the application through paid subscriptions.[5] And we're not talking about occasional users: paid Slack users spend more than 9 hours each workday connected to Slack and actively use it for 90 minutes each day. All told, Slack processes more than 5 billion weekly actions. According to an in-house survey, 87 percent of Slack users reported that "Slack improved communication and collaboration inside their organization."

Clearly, Slack answered an emerging need at just the right time. In an increasingly globalized world with a dispersed workforce, organizations didn't have a way to enable real-time conversations among their teams. Slack provides that and more, enabling users to search through messages for specific information and to include attachments, files, and links within their messages. In addition, Slack enables thousands of integrations with other tools and apps to increase collaboration and create bespoke functionality. According to a Slack survey, 95 percent of Slack users who use integrated apps find that those tools are more valuable within Slack than on their own.

It's worth noting that all of this utility has a side effect: each message, reaction, and integration creates records that are stored within Slack—and any of those records could end up being relevant to ediscovery or internal investigations. More importantly, traditional ediscovery and compliance tools were designed for email and other standard data types, not for Slack, which creates issues.

5. Elliott, Brian. "Not all Daily Active Users are created equal: Work is fueled by true engagement." Slack HQ (blog). October 10, 2019. Accessed August 7, 2020. https://slackhq.com/work-is-fueled-by-true-engagement

HOW SLACK DIFFERS FROM EMAIL

Slack operates like a constantly expanding digital bulletin board: anyone within a virtual "room," known as a channel, can see what's written there, regardless of whether they're contributing text. An organization might establish channels for:

- each active project it's managing,
- each team within a division,
- off-topic or personal conversations, and
- anything else it needs to keep organized.

Channels can be public or private

Channels may be either public, meaning they're accessible to anyone to join, or private, with a restricted audience. And Slack now allows shared channels through Slack Connect, where users from different organizations who are involved in the same project can participate in a single shared channel.[6] If users want to speak directly to one another outside of channels, they can send direct messages, either one-to-one or in small groups of up to nine users.

6. Slack Connect: A Better Way to Work With External Partners. Accessed August 17, 2020. https://slack.com/resources/using-slack/slack-connect

> Allowing editing and deletion of posts—especially if a record of that change isn't maintained—opens the door for users to intentionally or inadvertently alter, manipulate, or delete data.

Within channels or direct message feeds, messages typically accumulate chronologically. Because of this, a user—or an ediscovery reviewer—might need to read several screens of information to determine the full context for a given message. Additionally, users can choose to "reply" to an earlier message to keep that conversation thread linked to the original message.

We'll dive into this more in a moment, but one key to how Slack operates is its chronological, rather than topical, data structure within a channel or message history. By contrast, email data is more structured: all of the text of an email is contained within a message, which is itself contained within a mailbox. Anything that a custodian has sent or received can be found in that person's mailbox, unless they've deleted it.

Slack is like a bulletin board on steroids

By contrast, Slack's messages within a channel aren't organized into neat containers; they're simply piled atop one another in chronological order, like notes accumulating on a bulletin board.

So, since you don't have your own mailbox in Slack, how do you know when you have new messages to read? Slack users receive notifications when they're specifically mentioned (as @name) or when someone posts on a channel where they've enabled notifications. Slack also allows users to create groups, such as developers or managers. When that group is specifically mentioned (as @developers or @managers), Slack sends a notification to all of the members of the group. Users also receive notifications for direct messages they receive.

Users can also scroll through Slack to see what's been going on since they last checked in. Teams use channels to ask one another questions about their work, share helpful information or reminders, ask for and provide status updates, and generally discuss whatever project they're all working on.

Not that those conversations are limited to work. Most organizations establish informal "getting to know you" and social channels as well, allowing employees to connect around shared interests and strengthening the bonds within teams. In these days of social distancing, chatting on Slack can be one of the easiest ways for teams to stay personally connected regardless of time zones, work schedules, or other obligations.

Slack differs from email in another major way: by default, Slack allows users to go back and edit or delete messages that they've previously posted. Slack also gives organizations the option to preserve a record of such changes or to discard that information.

This is potentially a huge problem. Allowing editing and deletion of posts—especially if a record of that change isn't maintained—opens the door for users to intentionally or inadvertently alter, manipulate, or delete data. Sound familiar? That's the definition of spoliation, if it happens that the altered or lost data was subject to a legal hold and hasn't been preserved elsewhere.

On that note, let's turn to some of the challenges associated with using Slack.

UNDERSTANDING THE EDISCOVERY AND COMPLIANCE CHALLENGES OF SLACK

While Slack excels at its intended purpose—facilitating real-time collaboration—it raises some new issues and creates some serious data management challenges. Having a searchable log of every conversation your employees have ever had can rapidly become a liability from the perspectives of ediscovery, data privacy, and sound information management.

Data can become costly, potentially harmful, and of dubious business value

You may be asking yourself why keeping everything forever would really be so bad. At least you wouldn't be at risk of spoliation and its attendant sanctions, right? You'd have a record of every exchange you'd ever had about a given project, right there at your fingertips.

That's exactly right. And that might mean that you would have four years of Slack data—millions of messages—when you were served with a hostile workplace claim. Practically every one of those messages could be relevant to such a case. Not only would you be running the risk that there would be an old, but harmful, message in that archive, but you would also potentially have to pay to collect, process, review, and produce years of data and millions of messages, all with sufficient context for it to be understood. Risks like these are why data that is no longer useful for the business has no business hanging around.

This highlights, of course, the eternal tension between the demands of ediscovery and the business needs of information governance. These forces often act in opposition to one another, with the ediscovery side seeking to avoid spoliation claims by retaining data and the information governance side keen on deleting any data that isn't actively useful.

But the challenges of managing Slack data go a lot deeper than that, just as the uses of that data far exceed ediscovery.

POTENTIAL USE CASES FOR SLACK DATA

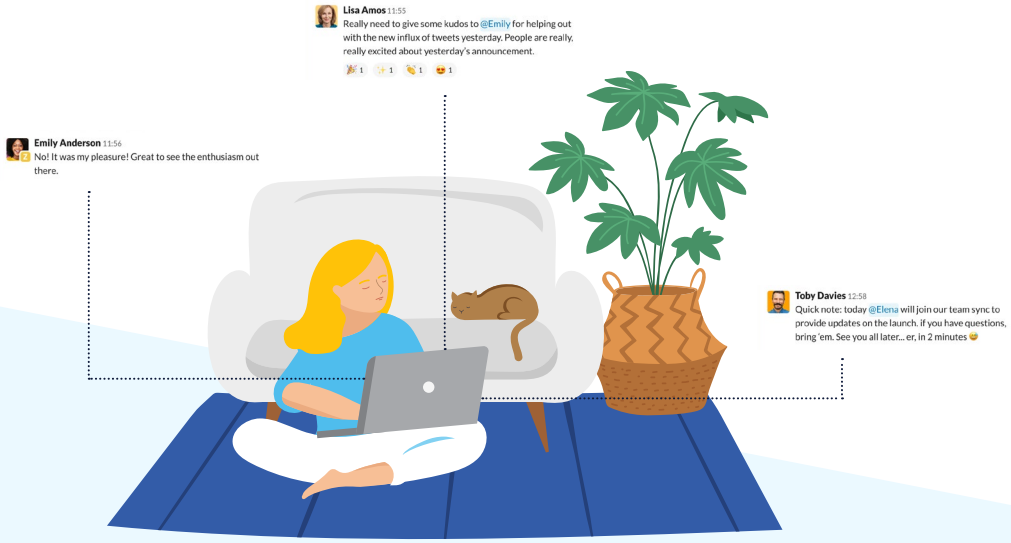
- Ediscovery and litigation response
- Regulatory compliance response
- Internal investigations
- Compliance investigations
- Cybersecurity response
- Privacy data subject access requests

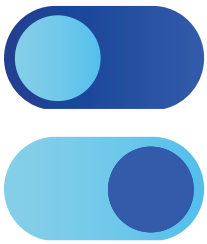
Slack may not be on the organization's information governance radar

As we mentioned above, Slack doesn't require any infrastructure or investment to start using it. This low barrier to entry means that many employees or entire departments simply adopt it without implementing any kind of institutional process or discussing its use with legal or IT. Due to these "guerilla campaigns," many organizations have been completely unaware that their employees were using Slack to discuss business. These companies eventually discover—often during a litigation matter or an internal investigation—that teams are having relevant conversations that haven't been collected or incorporated within their ediscovery or information governance pipelines.

Slack makes defining data custodians challenging

The flexible nature of Slack data makes it difficult to define custodians. With email, data is arranged into discrete packages of information and organized into separate “containers,” which makes custodians obvious. If an individual sent or received an email, she controls that information and is a custodian for it. Email boxes are like file systems: information is organized into logical and labeled units, and you can tell whose messages belong to whom. With Slack, that level of ownership exists with direct messages, but in channels, there’s also the concept of shared ownership of and access to information. These bulletin board-like channel communications, mixed together in the order that they were added, make custodian designations less obvious. It’s impossible to know whether a specific channel member read a specific message unless that person directly referenced it in another message. And the creator of a message can’t necessarily export or “control” that message like a typical data custodian could. In the same vein, the way that message context is dispersed within Slack raises questions about targeting the scope of an ediscovery collection.

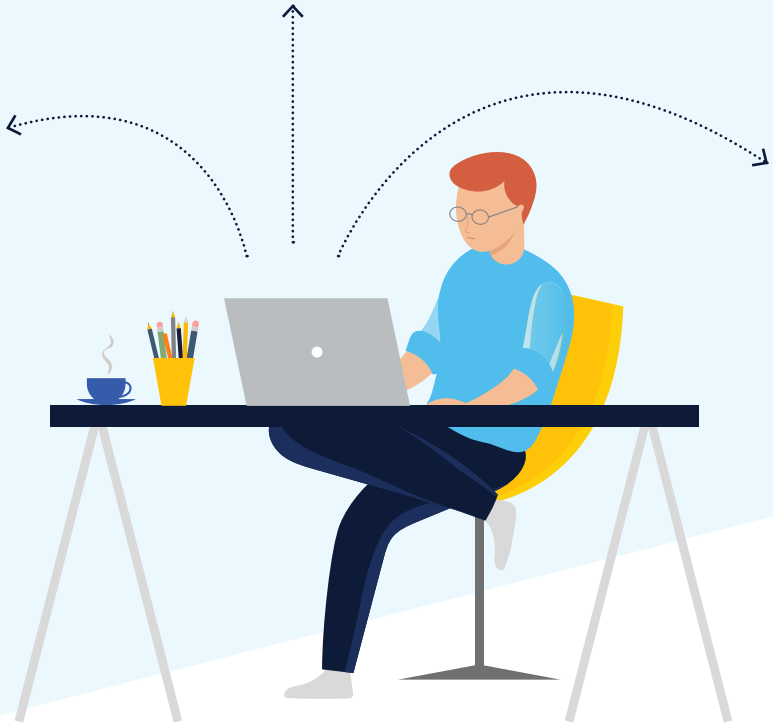




Slack's internal information management tools lack granular control

It's true that Slack has developed some tools and functions to address businesses' ediscovery and compliance needs, but at its core, it's a collaboration platform rather than an ediscovery or regulatory compliance tool. For example, recognizing the need to manage and defensibly delete data, Slack now allows users to set a data retention period, after which messages are automatically deleted. But that function isn't granular: it's either on or it's off. Optionally, an organization can allow users to set their own retention policies (i.e., override organization settings). Either way, specific information that's subject to a legal hold or a regulatory compliance retention requirement isn't sheltered and can't be preserved in place. At a minimum, automatic data deletion function can be turned off by setting the retention period, ensuring edits and deletes are logged, and preventing files from being purged if deleted by users. Clearly a lot of nuances that make preserving in place unreliable and risky.

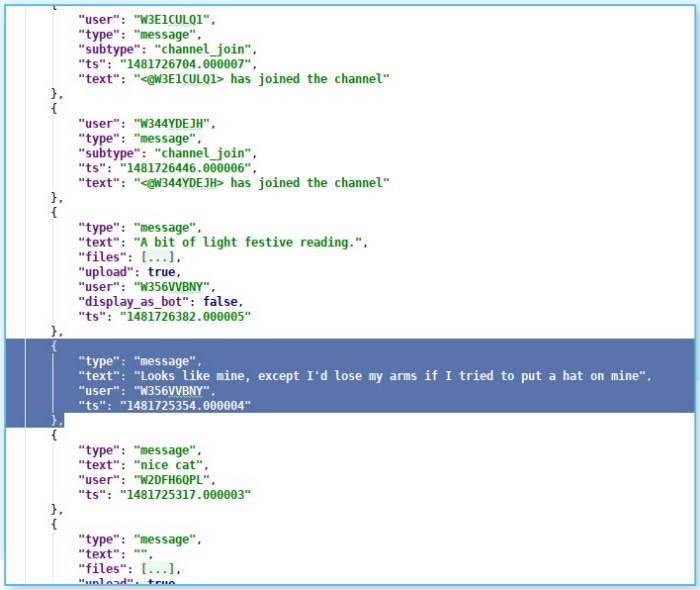
For organizations that juggle hundreds of legal holds, the result is that nothing can ever be deleted from Slack. In essence, Slack "solved" the information governance problem by introducing record retention settings—but that didn't solve the ediscovery problem. And of course, organizations using the free version of Slack only retain their most recent 10,000 messages, losing access to earlier data as they continue to generate more.



Slack's data exports are unwieldy

Similarly, the very nature of Slack data creates problems that the platform didn't anticipate. Efficient ediscovery review, for instance, is all but impossible. While Slack can allow certain authorized users to export data, those exports aren't targeted beyond limiting by date range. A further serious issue: Slack's exports are formatted as JSON files, which are not review-ready. JSON files require technical knowledge to extract into a useful form, and exports are generally only available for public channels. Each day of a channel generates its own JSON file, making it difficult to line up and correlate all messages or retain critical contextual information.

Obviously, using the default tools available directly through Slack precludes any precision in data management. Slack has created a discovery application program interface (API) to address some of these challenges, but the API is only accessible to organizations using Slack Enterprise Grid.



Slack's searchable, open format risks data privacy and confidentiality violations

Slack is wildly successful at its intended purpose because it's well-designed for sharing ideas and projects with a wide range of users. At any plan above the free level, it enables users to search all posts for specific information and to invite guests into conversations. The combination of these elements means that potentially sensitive or internal-eyes-only discussions can be inadvertently disclosed to external visitors. Add to that the casual, social nature of Slack and the sheer amount of time that people spend using it—again, the average user is actively engaged with Slack for more than 90 minutes each workday—and you've got a recipe for a breach of privacy, confidentiality, or both.

Companies with very mature litigation departments—generally serial litigants—or with sophisticated information governance, compliance, or investigations teams already have a good understanding of these risks and challenges. They may have already investigated an HR issue through their Slack channels, dealt with a privacy challenge, or had a data breach that required them to truncate their Slack communications. But most companies haven't addressed these challenges head on yet, because they haven't had to.

If you're struggling to manage Slack data, you're not alone. That's why we've created this straightforward guide to managing your Slack data.

MANAGE SLACK LIKE A PRO:

A STEP-BY-STEP GUIDE TO COLLECTING, PRESERVING, AND DEFENSIBLY DELETING DATA IN SLACK

Your Slack playbook should start with a clear goal: to preserve everything you need from Slack while deleting everything you don't need within a reasonably rapid record retention period. First, though, you have to know what you're dealing with.

1 TRIAGE AND INVENTORY YOUR SLACK DATA

You can't start to solve your Slack problems until you figure out what they are. If you don't know whether your organization is using Slack, start there. Add Slack (and other collaboration platforms) to your ediscovery custodian questionnaire and distribute it to everyone in your organization as part of your fact-finding mission.

If you know that you're using Slack—or if you find out about it during your early scoping —learn exactly how people are using it. What channels do you have in your workspace, both public and private? Who belongs to those channels? Do you have any shared channels through Slack Connect, and who are they shared with? What types of conversations are happening in various channels and via direct messages? Map out your workspace (or workspaces) and be mindful of context; Slack conversations can take a while to unfold, as people continue to add to ongoing discussions.

To expedite this process, consider adopting a tool that will intelligently determine where and how potential data custodians are interacting with the application. You want something that will generate a complete list of teams, channels, and users.

2 DETERMINE WHETHER YOU'RE USING THE RIGHT VERSION OF SLACK FOR YOUR ORGANIZATION

Now that you know where and how your teams are using Slack, it's time to compare your usage—and therefore your anticipated needs—with your capabilities, based on which version of Slack you have. While there is a free version of Slack available, few organizations will be able to satisfy their ediscovery, compliance, investigation, and other internal needs without the advanced features of a paid version.

Unless you engage in minimal, low-volume, low-stakes litigation and have few or no regulatory compliance demands or calls for investigations, we recommend upgrading to Slack Enterprise Grid. The only way to access fully functional ediscovery capabilities within Slack is through the discovery API offered via Enterprise Grid. Without it, plan to spend a lot more time, technical effort, and money extracting useful data from your Slack application.

3 DISABLE SLACK'S EDIT AND DELETE FUNCTIONS

Remember those message editing and deletion capabilities that we mentioned earlier? They're not doing you any favors. If they're enabled in your Slack (as they are by default), disable them. Even when message editing and deletion doesn't result in spoliation or regulatory noncompliance, those after-the-fact changes to a message can completely disrupt the flow of a conversation.

4 DEVELOP—OR REVISIT—YOUR POLICIES AROUND SLACK

If people are using Slack at your organization, you need to have policies in place to guide that usage. The very fact of adoption indicates that Slack is serving a useful purpose for your employees—especially if they're working remotely—so don't start a losing battle by trying to forbid its use. People enjoy the collaborative, rapid-fire communication that Slack allows, and for many companies, work happens faster and more effectively when workflows are freed from the constraints of email. Use your policies to set up checks and balances that will ensure the preservation of information in Slack for ediscovery, internal and external investigations, and compliance with regulatory record retention requirements.

- Strive to create clear, understandable, plain-language guidance that employees can and will comply with.
- Consider setting restrictions on who can create new channels or establish a process for creating and naming shared channels.
- Define who can add users, especially users from outside your organization.
- Set guidelines for appropriate communication style and topics within different channels for more efficient communications.
- Remind users that they are creating a written record and should always be professional and appropriate.

Slack has a casual, offhand feel, and it's easy for users to forget that everything they are writing is, in fact, part of their organization's data stores. The standard rule of "don't write anything you don't want to hear read aloud to a jury in court" definitely applies. Your Slack use policy is an excellent place to include this reminder.

5 ADD SLACK TO YOUR LEGAL HOLD NOTICES, CUSTODIAN QUESTIONNAIRES, AND CUSTODIAN INTERVIEWS

Incorporate Slack into your ediscovery process, beginning with your legal hold notices and custodian inquiries. In fact, don't limit this to Slack: make sure that your hold notices and questionnaires encompass all collaboration or project-management platforms that your teams are using so that you're not caught off guard by an unexpected data source.

Although employees won't be responsible for preserving their own Slack conversations—more on this below—clearly notify them that their messages within Slack may be relevant and discoverable. Use your custodian questionnaires and follow-up interviews to investigate what communication platforms your custodians use, and get specific. What channels are they active in? What channels do they rarely access? What discussions have they had on those channels or in direct messages? Use your questionnaires and interviews not just to gain information but also to remind custodians about additional data sources.

6 EDUCATE ALL PERSONNEL ABOUT YOUR SLACK POLICY AND WHY IT'S IMPORTANT

Chances are that most of your employees aren't ediscovery professionals. They don't wake up in the middle of the night in a cold sweat, worrying that they may have allowed the spoliation of case-dispositive electronically stored information. So educate them about the risks, not just once but repeatedly. Don't assume that they've read and fully digested every one of your policies. Offer continued training about the risks of undisclosed information sources, the reasons you've established certain policies, and the penalties for spoliation of evidence. Spell out exactly how they can comply with best practices around Slack.

7 SET RULES FOR DEFINING CUSTODIANS AND ESTABLISHING THE SCOPE OF DISCOVERY WITHIN SLACK

Remember that custodians don't have a straightforward definition in Slack the way they do with email. Ordinarily, a custodian has direct control over information in their possession. With Slack, by contrast, individual users have very limited control over their channels and do not "possess" information in the traditional sense.

When you're looking to capture data for a specific person, you likely need to capture messages from every channel that person used or was a party to, regardless of whether they were active there. Like a physical bulletin board, Slack doesn't monitor who has read its messages. Therefore, it's safest to impute knowledge of all of the data in a channel to every member of that channel.

Slack requires a new approach to determining the scope of discovery or a fact-finding investigation as well. Because Slack conversations present information in a free-flowing chronological format, you'll rarely be able to convey the full context of a message without capturing the surrounding messages. You'll likely need to be flexible and adaptive as you define how you will collect, search, and review messages to identify those that are relevant to a matter, but try to set some ground rules to guide you in making that determination. Again, look for a specialized tool that will help you in defining and managing the scope of an inquiry.

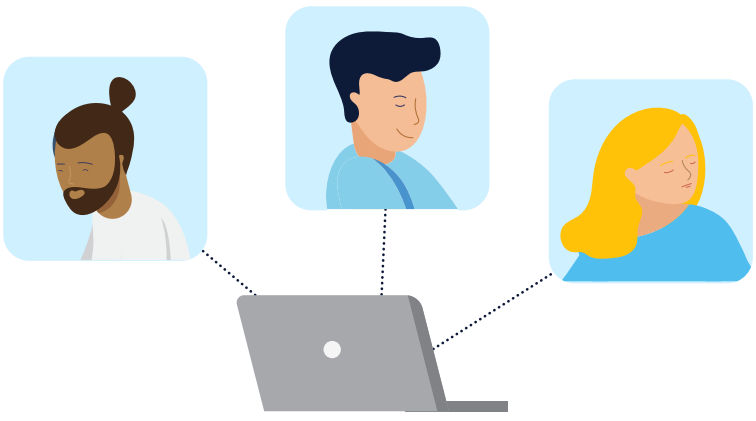
8 PRESERVE DATA BY COLLECTING WHAT YOU NEED AND STORING IT OUTSIDE OF SLACK

Now we get to the thick of it: how do you comply with ediscovery and regulatory compliance obligations—and save relevant information during the course of an investigation—without keeping all of your Slack data forever? The key is to defensibly preserve that information outside of your Slack application by exporting it in a workable format. Slack doesn't allow for in-place preservation of select messages; again, its data retention setting is pretty much binary, either on or off across an entire channel or workspace, rather than granularly targeted to specific information. For our purposes, we'll discuss preservation and collection as a single process for Slack data.

As we discussed earlier, there are two ways to export Slack data to preserve and collect it: using Slack's Corporate Export to generate JSON file exports, or employing Slack's discovery API enabled through Enterprise Grid. JSON files are untenable for serious ediscovery due to their format and the difficulty it causes in reviewing messages and the lack of being able to target specific information for export—presenting excessive data to sift through. We advise that if you need Slack data for discovery, you need the Discovery API.

Look for an ediscovery application that allows you to place individual Slack users on hold and capture both their historic and ongoing content with enough context to make sense of individual messages. Additionally, you want a solution that allows you to view data with its surrounding information as it appeared in Slack, including automatic updates of ongoing conversations and additional information. This is part of why Slack's exports, which create a new JSON file for each day's activity within a channel, are an unwieldy approach to ediscovery, especially when it comes to review.

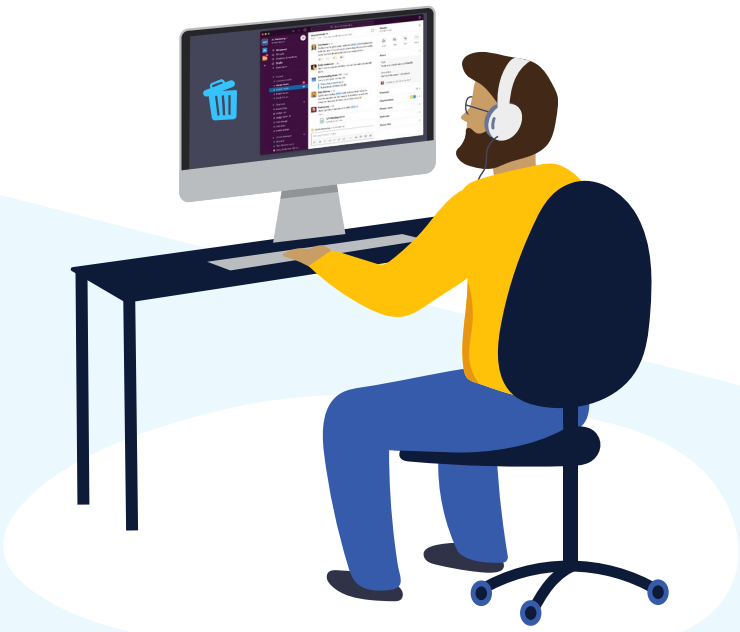
When you create a targeted, immutable archive outside of Slack, supported by an audit log, you also solve the tension with information governance: Slack can still delete data according to an established record retention schedule while everything subject to a legal hold is retained separately and defensibly.



9 ENABLE AUTOMATIC MESSAGE DELETION

Once you're preserving potentially relevant messages outside of Slack, it's time to eliminate everything that isn't serving a continued purpose. Remember that Slack's basic functions don't include ediscovery or regulatory compliance. That's why the easiest approach is to separate those functions from Slack, exporting to preserve any data that's subject to a legal hold, relevant to an investigation, or required for regulatory compliance. That way you can keep an automatic deletion process operating within Slack, minimizing the risks associated with outdated information that no longer offers any business value, while ensuring compliance with all of your legal obligations.

As part of your Slack policies and guidance, consider directing all casual, non-work-related conversations to designated channels or direct messages. You can then implement a tiered retention schedule that deletes those messages more frequently while keeping mission-critical information in channels with longer retention periods.



10 BE MINDFUL OF THE CONTEXT OF MESSAGES AND PLAN AHEAD FOR REVIEW

As you establish your Slack collection process for ediscovery, investigations, and regulatory compliance, keep the end goal in sight: review and production of relevant evidence or production of requested information to a regulator. If your solution allows you to export data and store it but you still can't decipher that data or navigate it easily, review—already the costliest stage of ediscovery or any other fact-finding mission—will be even slower and more expensive. Ensure that your preservation and collection process provides you with an output—a coherent, integrated view of your Slack data in its full context—that allows your review team to do its job smoothly and efficiently.

11 USE SEARCH FUNCTIONS AND A DISPLAY THAT ENABLES COST-EFFECTIVE REVIEW

To be fully useful for ediscovery, your Slack exports can't just be pretty; they also need to be in a searchable text format, complete with supporting metadata for authentication. Look for a solution that enables search functions by author, channel, keyword, and date range, at a minimum. Additionally, you should be able to review messages in context without jumping from file to file. The easiest approach is to use an export format that can be directly loaded into an ediscovery review platform like Relativity.

12 PLAN FOR THE RELEASE OF LEGAL HOLDS

You should always have an exit strategy for legal holds: a defined process that kicks in when a matter has been resolved or otherwise ended to return data under an expired legal hold to your defensible deletion pipeline. This process ensures that you'll stop collecting data, extract any useful institutional knowledge from the data you've gathered, and evaluate the data itself according to your standard record retention protocols. If you've set up a preservation and collection solution that operates entirely outside of Slack, you can just delete the collection when your obligation to preserve that information ends. Any data that's not yet expired under your record retention guidelines will still be within Slack and on schedule for destruction at the appropriate time.

There you have it: an overarching view of the advantages of using Slack, the ediscovery, investigation, and regulatory compliance challenges of doing so, and a step-by-step guide to implementing Slack such that you can gain the advantages of this extraordinary collaboration platform without suffering the challenges. We're big fans of Slack here at Hanzo, and we're confident that our Slack collection technology is the best in the industry. To find out more, contact us.

ABOUT THE AUTHOR

Brad Harris, VP of Product, Hanzo

Brad Harris is the VP of Product at Hanzo, a pioneer in the contextual capture, and preservation of dynamic web and collaboration content for corporate legal and compliance departments. He leads product vision and innovation for the company. Brad has more than 30 years' experience in the high technology and enterprise software sectors, including assisting Fortune 1000 companies enhance their e-discovery preparedness through technology and process improvement. Brad is a frequent author and speaker on data preservation and e-discovery issues and is a member of The Sedona Conference WG1 and WG6.

hanzo

Hanzo is solving the biggest challenges in legally defensible compliance and litigation today—contextual investigation, collection, and preservation of web-based dynamic content as well as Slack data, including messages, notifications from integrated apps, and file attachments. Through one sophisticated platform, Hanzo captures and preserves team messaging data, social media engagement, and interactive web content, then archives it for analysis and review in a legally defensible native format. Launched in 2009, Hanzo serves government agencies, enterprises, and top law firms across the globe.

Ask for a demo to learn more about how Hanzo can help your organization set up their own Slack at hanzo.co/contact-hanzo.