THE NEW E-DISCOVERY WILD WEST: SLACK, TEAMS, ZOOM, AND OTHER COLLABORATION TECHNOLOGIES

K&L GATES

Contributing Authors:

Julie Anne Halter, Partner and e-Discovery Analysis and Technology (e-DAT) Practice Group Coordinator

Kelli Fiesta, Lead e-DAT Senior Staff Lawyer

Michael Goodfried, e-DAT Senior Staff Lawyer

Sheila Phillips, e-DAT Senior Staff Lawyer

Gina Marie, e-DAT Staff Lawyer

Sean Selin, e-DAT Staff Lawyer

Clinton Field, e-DAT Team Lead

It goes without saying that the COVID-19 pandemic fundamentally changed the way we live and work. As many organizations have moved from an in-person to a hybrid or fully remote work force, the business communication applications that were the mainstays of pre-pandemic work life—email, phone, fax, paper, and simple instant messaging programs—have been increasingly supplemented, if not supplanted, by business collaboration technologies. While these collaboration technologies are not new, their adoption in the workplace (whether formally sanctioned by a workplace IT department or not) dramatically accelerated during the pandemic. This acceleration has fundamentally altered the type, volume, and nature of the communication landscape.

Collaboration technologies, such as Slack, Microsoft Teams, Zoom, and scores of others, certainly allow employees to communicate with one another more easily. But another reason for their increasing popularity is that they create a one-stop shop for end users, seamlessly integrating the ability to perform other tasks as well. For example, from within a single collaboration application, an employee can co-edit a document, search for reference material, hold a virtual video meeting, review and respond to comments in a group chat, engage in private 1:1 conversations, and interact with an HR bot to schedule a vacation. Moreover, these applications offer a centralized, "always-on" connection through a familiar, user-friendly interface. In a way, then, these tools provide employees with functionality that allow for more informal and idiosyncratic interactions, which more closely mimic the collegial feel of prior, daily in-person communications.

The relaxed tone and tenor of communications that occur within these collaboration applications is often a welcome reprieve from the formality and structure of more traditional forms of business communication, such as email. The business use of email, however, has evolved over the years. Many employees have long been sensitized to the lasting nature of formal business communications and take great care to write thoughtfully and judiciously. Numerous continuing legal education classes have warned of the email discovery adage—if you don't want to see it on the front page of the New York Times (or as Exhibit 1 to your deposition), do not put it in email! With these more informal collaboration applications, however, employees seem to have forgotten or maybe just fail to appreciate that— just like any other nonprivileged communication—chat box comments and all of the other communications that occur within these collaboration technologies are likely not private, and are absolutely discoverable.

So while the benefits associated with keeping employees meaningfully connected and engaged with one another cannot be overstated, particularly in today's hybrid work environment, for in-house and external legal teams, the explosion of these types of communications can create significant new challenges. In an ideal world, an employer could simply set the rules and assume that employees are using only those technology applications provided or sanctioned by the organization's centralized IT department and incorporated into the organization's information governance policies. But in many organizations, employees will find the path of least resistance, and if the organization doesn't provide the technology needed to most efficiently do

business, employees will find and implement it on their own. In many respects, it is a new "Wild West."

For these reasons, every organization's near-term "to-do" list must include an effort to determine what applications the various business units, departments, or teams are using; where they are being used (e.g., mobile device or laptop); what types of data these applications are generating; where that data is being stored (if at all); and to whom the data is (or should be) attributed. Doing so will help your organization better protect and profit from company intellectual property, comply with data privacy laws and regulations, investigate employee complaints or other matters, and respond quickly and efficiently in litigation. Once you know what types of collaboration applications are being used in your organization, and how they are being used, your organization will better understand the potential risks of using that technology, assess whether those risks are acceptable given the efficiencies gained, and begin to tame the Wild West.

COLLABORATION TECHNOLOGIES: A DISCOVERY BAG OF NAILS.[1]

One important area where collaboration technologies can present significant risk is in discovery. The federal rules of civil procedures and their state-court counterparts were amended in 2007 and 2015, specifically to account for evolving technology in the work place and beyond. It would seem logical, then, that practitioners would simply apply these same rules to collaboration technologies. But it is not quite that simple. Collaboration technologies differ from traditional business tools in a number of fundamental ways that make traditional e-discovery concepts and norms less clear. For example, in the context of collaboration technologies, common e-discovery concepts such as "author," "custodian," a conversation "thread" and even what constitutes a "document" have materially changed.

Who or what is an author or custodian?

In litigation, electronically stored information (ESI) orders often refer to the concept of a custodian as a surrogate for Civil Rule 34's that documents be "produced as maintained in the ordinary course of business."[2] But when ESI created in collaboration technologies is at issue, the concepts of who is a custodian or an author of particular ESI became sixes and sevens.[3]

Traditionally, the author of a document has been the original creator or the last person to update an iteration of the original. Employees often saved files to their company-issued hard drives or to a small number of dedicated network locations or document management systems, so searches for a custodian's ESI[4] were relatively straightforward. When collecting data for litigation purposes, email accounts and network folders were the most common sources and provided the bulk of the data.

In a collaboration application, however, multiple users may simultaneously edit the same document. The document may be saved with the author listed as one of the many contributing editors, but that information may not be an accurate representation of the author for litigation purposes. In such instances, it may not be possible to identify the author of a particular document. Thus, understanding the limitations of the technology in certain circumstances means you are better able to proactively identify and confirm the information you may need to comply with Rule 34's various production requirements.

Similarly, while direct user-to-user communications are still possible within collaboration technologies (e.g., direct chats), these technologies also facilitate easier one-to-many communications. For example, users who post to a group chat or "channel" are, in effect, communicating with anyone and everyone who has access to that channel including, potentially, anyone in the company. This concept is very different than traditional email where the author chooses to direct their communications to specific recipients.

Consider, for example, that employee John Doe is a member of 350 different channels on a variety of work-related topics within his organization, many of which have existed for years. Although John reads all of the posts, he comments only semi-regularly. If John is an identified custodian in litigation, which of these 350 channels must be preserved, collected, reviewed, and produced to respond to discovery requests? Certainly, the preservation obligation is likely limited to those channels that are reasonably likely to have content that is relevant or responsive to the discovery requests or to the claims and defenses in the litigation. But beyond that, is it only the messages that John has posted that must be preserved, collected and reviewed? What about the messages to which John has responded? Aren't they needed for context? Should the legal hold, collection and review obligation include every single message in every channel? In that case, do the other employees involved in the channel discussions need be added to your custodian list?

Alternatively, consider that employee John Doe posts a document to a shared workspace to be edited and refined by colleagues. Multiple people review and revise the document over time and the finished product looks very different than the version that John originally posted. Is John the author of

the document in the traditional e-discovery sense? Is he the custodian of the document? If not who, or what, is?

In short, for those of us who practice in the discovery and e-discovery fields, it is important to recognize and appreciate that collaboration technologies fundamentally alter the way we may need to think about some basic e-discovery concepts. The right approach may differ from situation to situation, particularly given the amount of data that could be implicated, so practitioners will be well-served to consider and discuss these issues in advance to make sure that discovery proceeds efficiently and cost effectively.

What is a document?

Perhaps the biggest difference between the data generated using traditional communication tools (like email communications or the rare internal memorandum) and those generated using collaboration applications is what constitutes a "document" for purposes of your Civil Rule 34 discovery obligations.

Within the collaboration application environment, communications often occur in one, continuous scrolling window. Determining where a particular communication begins and ends from within that continuous set of communications can be more art than science. This is particularly true since many of these channels have hundreds of users, and communications can occur over a period of weeks, months, and years, and encompass a wide range of topics.

When faced with litigation, organizations and practitioners must consider the extent to which these conversation threads must be preserved, reviewed and ultimately produced. In other words, they must determine whether, under Civil Rule 34, the responsive or relevant "document" that is subject to preservation and production obligations consists of the entire conversation thread or only some portion of it. If the former, you may find that the vast majority of communications within the thread are not at all relevant to the claims and defenses in the matter, and give rise to other important considerations such as privilege and confidentiality that require careful, individualized review. If the latter, how do you determine what portions of the thread will be produced, and who gets to make that decision?

When it comes to these types of chat messages, one way to define a "document" is to include all messages within a specific chat group on a given day. Especially given their typically informal and truncated nature, context is often very important to correctly interpreting a chat conversation. Individual chats taken out of context can be vague, misleading, and intentionally or unintentionally misconstrued. But given the rapidly increasing number of communications within our organizations using these collaboration technologies, the number of messages that could potentially be implicated is staggering, and the cost of addressing them in litigation may not be reasonable or proportionate to the needs of the case. One reasonable approach is to treat all the chats within a given channel on a given day as the "document." Of course, chat conversation threads can extend across multiple days, but it may be easier to keep the single-day document definition and join multiple day documents where needed.

The group chat and channel functionalities available in tools like Slack and Teams have capabilities beyond just sending chat messages[5] that give rise to additional challenges when it comes to defining a "document." For example, an employee replying to a chat message can send an embedded file or a link to a document on a separate server. In the context of email communications, an embedded file constitutes an attachment such that it, along with the parent email, is considered a single compound document. But what about chat messages where there is no physical attachment, but rather a hyperlink to content stored outside the chat environment. Is the content found at that link part of the "document" even though it is outside of the chat environment? At least one court does not think so,[6] but the facts and circumstances of that case, including the practical difficulties associated with searching for and collecting content at embedded links,[7] along with a negotiated ESI protocol were important and determining factors.

Collaboration technologies also offer the ability to communicate during video meetings through the use of virtual white boards and sidebar chats. These white boards and sidebar chats may be saved as part of a meeting recording, or saved separately by individual meeting participants. Should such white board content and sidebar chats be considered attachments to a recorded meeting to form a single, compound document? What if the meeting recording, the white board content and the side bar chats are stored in different locations? As the lawyer responsible for document discovery in a particular matter, how would you even know that the white board content and side bar chats exist, or that they were in some way related to the original meeting recording?

Similarly, collaboration technologies also offer the ability to share files easily and efficiently across users: spreadsheets, presentations, memos, and other files; recorded webinars and meetings; and calendar items. Each of these files can be generated or shared from within the collaboration application, and chat group members have access to all files

associated with that group. In this context, are documents created in separate, but linked, applications to be considered stand-alone documents? Or should they be treated as attachments to a channel such that they are all part of a compound document? While these questions may be seen a theoretical, courts have made it clear that data generated within collaboration applications is subject to discovery.[8] And these are the tools our clients are increasingly using to communicate and to perform their job functions. As practitioners, we must carefully consider how we will advise our clients in dealing with these new data challenges or find ourselves bad boxed.[9]

What data is even available to your organization?

Given their ease of use and transitory nature, many employees consider the communications that occur within collaboration applications as somewhat ephemeral. Legal and regulatory requirements, however, generally do not. When an organization reasonably anticipates litigation or another event triggers a legal hold obligation, potentially relevant data generated using collaboration applications is subject to that obligation. For that reason, it is critical that organizations have a firm understanding of the retention policies and settings associated with that data.

Of course, as organizations scrambled to find meaningful ways for employees to stay engaged and connected during the pandemic, many were quick to embrace these new technologies, but did not necessarily have the time or resources to think through the information governance and records retention issues before employees jumped in. As a result, some organizations may be operating under default data retention settings based on the nature of their license agreement with the collaboration technology provider. These settings may not align with the organizations' information governance policies and could leave them vulnerable to data disposition issues if a dispute arises.

As organizations attempt to wrangle these issues, they must analyze the data retention settings for their various collaboration applications and modify them, if needed, to ensure the desired result. In general, organizations should:

- Adapt any existing retention policies to cover data generated using collaboration applications;
- Keep collaboration data for the shortest period of time possible (unless subject to legal hold);
- Tailor any retention to the smallest unit (department, chat group, user) possible;
- Consider all of the potential types of data and the specific policies that data may trigger (e.g., regulatory requirements, employment, trade secret confidentiality and protection); and
- Devise a policy that applies to data generated before the updated information governance protocol is adopted.

Unfortunately, these information governance guidelines often run counter to the way the collaboration applications are configured. For example, the default retention settings in Slack, and similar technologies, is to retain all messages and files for the lifetime of the workspace (except in the case of free accounts).[10]

It is imperative, then, that organizations create information governance policies, conduct employee user training and communicate appropriate use and storage standards for this technology in order to establish a reasonable business and legal framework for their deployment. Such policies, procedures and training, however, will not likely be sufficient when faced with claims of spoliation or the like. Organizations must also understand and implement appropriate technological safeguards, such as blocking access to certain applications or application features, or controlling the back-end settings of an application so that users may only deploy it in the desired configuration.[11]

How do licensing terms impact these issues?

As if all of this were not complicated enough, an organization's software licensing can impact how customizable these back-end data retention settings actually are. For example, organizations using Slack have access to their users' data based on their licensed level of service. For free accounts, the accessible message universe consists of the 10,000 most recent messages (though Slack retains all workspace data on the back end). Higher levels of licensing include the ability access to public channel content, including access to files, but not private channels or multiparty messages. Corporate accounts often include greater levels of access, and offer the ability to filter to and export messages of particular interest, but even the level of available filtering is based on the selected corporate Slack license plan. Finally, in Slack, workspace owners are able to specifically configure and customize the retention settings, but only if the company has a paid subscription. Thus, another important action item for organizations using collaboration technology is to understand the applicable levels of retention, search capability, and export before litigation or some other form of compulsory process forces upgrade licensing negotiations.

What about legal hold obligations?

Along with understanding the nature and extent of available collaboration data, it is also critically important to understand how your organization will implement a legal hold, as well as collect and export potentially relevant data, before a dispute arises. When working with collaboration technologies, identifying, preserving, searching, collecting, and attributing the data to an appropriate custodian often opens a whole can of worms.

As a preliminary matter, it is important to understand what collaboration technologies your organizations are using, but it is equally important to understand how they are using them. That information will help inform whether a particular type of data is likely to be relevant to claims or defenses in litigation.

Once you have identified the data sources and types that need to be preserved, you must decide what content will be preserved. Will you attempt to preserve everything (which may be easy in the short term, but which could be cost prohibitive when it comes to review and production) or will you attempt to use filtering criteria to limit the universe of data to be preserved? If the latter, organizations must have some reasonable basis to know which applications are being used on what devices and what language is spoken by the users of those applications.

For example, with collaboration applications designed to facilitate instant and less formal communication, the use of truncated sentences and abbreviations are the norm,[12] as are use of emojis and GIF files. The true meaning of words, phrases, or images could be opaque to an outsider or to someone who simply was not chat group participant. In those circumstances, it may not be possible to use traditional search terms to identify potentially relevant data. Moreover, it may not even be accessible without intermediate steps to extract and de-code the data. For instance, a GIF file that contains text embedded in the image would not be searchable without separate processing and the creation of OCR, and even then, may still not yield searchable results.

When considering an organization's legal hold obligations, it is also important to recognize that the same data may exist in the custody of different employees. Consider a recorded virtual meeting with 10 participants. Each participant may use a different meeting layout, with or without the chat window open. While Buck is presenting about the topic at hand, two employees, Dolly and Wyatt, are exchanging a series of private chats, while Dixie is broadcasting her chat comments to the entire group, sending the attachments as well as links to other documents referenced in Buck's presentation. In this context, which version of the meeting is stored? Which version(s) should be preserved? Is there metadata recorded that allows a particular saved version of the video to be traced to the individual participants? Does the collaboration application keep a record of the multiple, independent chat threads? Does it keep a record of the documents shared within the chat? What about links to documents outside of the chat but within the organizational network? If recordings are collected for purposes of litigation, what information will be available to you and will that be sufficient to meet your discovery obligations? Further, if each of the participants has the ability to record the meeting, is it necessary to produce all versions of the recordings because they contain similar, but slightly different versions (e.g., screen layout, private chat information)? If the company is storing a copy of recordings for each participant, how will the company keep pace with the storage requirements? If a question arises regarding the content of the virtual meeting, does your license level allow for the automated creation of searchable transcripts? If not, and you are unable to keyword-search the recorded file, have you considered how you will determine whether the recording may contain relevant content?

Given these complexities, practitioners must recognize that traditional legal hold processes—such as sending out written legal hold notices to identified custodians—may no longer be sufficient when collaboration application data is implicated. In certain circumstances, it will be critical to take affirmative steps to update relevant retention settings to prevent any automated deletion of data under legal hold. In other circumstances, multiple software applications may interact behind the scenes of the collaboration application, such that each must be individually analyzed to determine whether and how their settings may impact data retention. Moreover, because these tools are relatively new in the e-discovery industry, collaboration technology software developers may not have fully implemented or even considered a legal hold interface or offer legal hold capabilities for your organization's licensing level.

How is collaboration data collected, processed, and reviewed?

Assuming you have successfully preserved the relevant collaboration technology data for your legal matter, absent early resolution, there will come a point where that data must be collected, processed, reviewed, and produced. As with other phases of the EDRM, collaboration technologies present challenges during this phase as well.

Data Export Format

Some collaboration applications, Slack being the most prominent, currently permit data exports only in a (nonuser friendly) structured data format. Specifically, Slack exports can only be made in a data format called JSON which, depending on the litigation support system used by you or your outside counsel or vendor, generally requires additional processing before it can be analyzed.

At the time of export, it is also important to validate that you have received complete and accurate metadata for all collaboration data at the time of collection. The failure to receive accurate metadata can have significant downstream consequences. For example, Slack attributes a particular message to a particular user using a random alpha-numeric User ID. These randomly generated User IDs, which do not reference the user's name, are the primary means by which a Slack message is assigned to a particular custodian. The ability to cross-reference the Slack-assigned User ID to the custodians or witnesses in your matter is a critical aspect of litigation discovery.

Similarly, accurate metadata is also critical to determine the date messages were sent, how they were sent (public or private channel, direct, or multiparty message), and whether or not the message referenced a link or attachment, all of which may be useful information to properly scope the collection, review and production strategies and workflows. For these reasons, it is important to formulate a plan for how you will process and review Slack data collections before the collection process even begins.

Teams is also unique in the way it treats chat messages upon export. Under most Teams licensing levels, chat messages are not exported like threaded email. Instead, each individual message is rendered as an individual, stand-alone communication. As a result, using search terms as a mechanism to identify data for collection or review will likely yield insufficient results. Although search terms will capture a stand-alone communication that contains one or more of the terms, they will not capture any related messages for context unless they, too, contain one or more of the search terms. As noted above, while at first glance, a message may not seem particularly important, that single message could suddenly take on new relevance in light of the 10 or 20 messages surrounding it. Moreover, as described above, Teams messages often contain links to content stored outside of the messaging environment in a variety of different locations (as opposed to attachments). It is often not possible to determine which external locations may contain relevant links until after the message review is complete.

Other messaging or messaging archiving systems, such as Google Workspace or Smarsh®, tend to use more common export file types, but even these more common file types can trip up less seasoned e-discovery practitioners. Teams messages are often exported in a very common PST format, and are therefore easily processed and loaded into standard litigation support and document review platforms. However, once the Teams messages are loaded into a review platform, it is critical that specific metadata for those messages is also available within the review tool so that the end user is able to review the chat messages in some form of order. Spreadsheet or .csv exports are a common format for chat messages exported from mobile devices through Cellebrite or other phone imaging software, but these tend to be more easily reviewed outside of a standard document review platform.

Licensing Levels

We previously noted that licensing levels for collaboration technology can impact the type of data users can create, as well as where and how it is stored. Licensing levels can also impact what data is available to collect, and how it is collected. For organizations leveraging Teams, for example, chat data is available for export and collection under most business licenses. Threaded chat data, however, is only available at the highest licensing level. Understanding this potential limitation in advance is important because, as noted above, viewing chats in a threaded context is sometimes the only way to properly interpret their relevance, and may be the most reasonable way to produce them.

Attempting to Tame the Wild West

As the e-discovery industry grapples with this new type of relational collaboration application data, some software companies have stepped in to help. These companies have built third-party connector applications that can help bridge the gap until traditional e-discovery platforms are able to fully incorporate efficient processing and review workflows into their existing tools. Slack, in particular, encourages organizations to collaborate with their e-discovery partners for collections and processing. Although Microsoft has focused on building its own discovery modules, it also provides connector access (via an API) to its Microsoft 365 environment for third-party e-discovery software such as Nuix and Relativity.

As a practical matter, the ability to leverage these connectors generally requires an administrator's level of access privileges and setup work. This high level of access permissions can make it difficult for external firms to use these tools on an ad hoc basis, but they can be very valuable

resources for clients who implement them directly. For all the reasons outlined above, when working with clients who directly deploy these connectors, in-house and outside counsel must be familiar not only with the underlying collaboration technology, but also the connector and how it searches, collects, and exports messages and metadata.

In short, currently available litigation support tools were generally built to handle email and more traditional forms of communication and documents. Many are working hard to make changes to better support the processing and review of collaboration application data. But not every platform has full support for the major data types, and it is unlikely that any single platform will be able to handle every proprietary collaboration application messaging system which currently exists. As such, it is important to consider the implications of these issues in our clients' matters early, so that we can plan for and execute discovery protocols that help to tame the collaboration technology wild west.

The Next Frontier

Collaboration technologies and the data they generate really are the next frontier in the legal e-discovery industry. While in-house and outside counsel are not required to be experts, it is critical that they understand basic concepts about these emerging technologies, how they are used, the data that is created, as well as some of the limitations of existing e-discovery technology to identify potential traps for the unwary and reach out early in the process for technical assistance.

To stay current, consider keeping abreast of the collaboration applications available and those being used by employees or by an industry. Doing so does not have to be a complicated research exercise. Just ask your clients. Find out what tools they are using and how they are being used. Ask what level of service or licensing agreement they have, and then find out whether or not they have adopted or implemented information governance policies and procedures. In parallel, make sure you have a good working relationship with an e-discovery professional who knows how to efficiently and cost-effectively address this collaboration data under these circumstances, should litigation or other matters require it. Armed with these basic data points and supplemental resources, your next e-discovery project is much less likely to be a showdown at the O.K. Corral.

---

[1] Bag of Nails – A cowboy expression that means "chaos" or "confusion." https://coloradotrails.com/blog/top-100-cowboy-expressions-and-phrases

[2] See, e.g., Heartland Food Products, LLC v. Fleener, 2019 WL 2501862, at *3 n.22 (D. Kansas June 17, 2019), citing David J. Kessler & Daniel L. Regard II, Format of Production, THE FEDERAL JUDGES' GUIDE TO DISCOVERY EDITION 3.0 186, 189 (The Electronic Discovery Institute, 2017) ("Rule 34(b)(2)(E)(i) makes it clear that "a producing party has the discretion to produce the documents as they are organized in the ordinary course or to produce them by document request.... Generally, a producing party produces emails in the usual course when it provides sufficient information about the email, typically including the custodian for the email, information to link emails with attachments, and the date and time the email was sent or received"; Venture Corp. Ltd. v. Barrett, 2014 WL 5305575, at *3 (N.D. Cal. Oct. 16, 2014) ("Providing information about how documents and ESI are kept under subsection (i) "[a]t a minimum … mean[s] that the disclosing party should provide information about each document which ideally would include, in some fashion, the identity of the custodian or person from whom the documents were obtained …" (quoting Pass & Seymour, Inc. v. Hubbell Inc., 255 F.R.D. 331, 337 (N.D.N.Y. Sept. 12, 2008))).

[3] Sixes and sevens – A western expression that means "to be in a state of disorder or confusion." https://www.legendsofamerica.com/we-slang/13/

[4] When the Federal Rules Committee crafted the term "electronically stored information" it was designed to be intentionally broad so that it could encompass technologies that hadn't been invented yet. The discovery concepts that are applied to email and other files may also be applied to newer collaboration technologies such as Slack or Teams. Those concepts may, however, need some adjustment in order to facilitate create an efficient and reasonable discovery process.

[5] A group chat/channel is a place where employees can share information, conversations, tools, and files. For example, in Microsoft Teams, a general channel is available to every Team. Group, departmental, divisional, or company-wide information can be shared via the Team's general channel. Additionally, each Team can create multiple channels tied to specific projects, tasks, events, or just to engage in morale building activities. These channels can be private, shared, or include guest Team members from outside the company.

[6] Nichols v. Noom, Inc., No. 20-CV-3677 (LGS) (KHP) (S.D.N.Y. Mar. 11, 2021).

[7] In fact, in certain circumstances, the linked content may have been updated or changed since the link was originally sent, or the linked content may no longer exist.

[8] Not surprisingly, courts interpret Rule 34 to find that Slack data is subject to discovery when the propounding party can demonstrate that the data is relevant to any party's claim or defense, not privileged, proportional to the needs of the case, and within the responding party's possession, custody, or control. See Laub v. Horbaczewski, 2020 U.S. Dist. LEXIS 247102, at *11–13 (C.D. Cal. Nov. 17, 2020) (finding that the plaintiffs credibly argued that certain private Slack messages may be relevant because the messages would show evidence of the underlying contract violation claims, but concluding that the defendant did not have "possession, custody, or control" over the private Slack channels under the free version and standard version of Slack); Milbeck v. TrueCar, Inc., 2019 U.S. Dist. LEXIS 165649, at *4 (C.D. Cal. May 2, 2019) (finding that Slack messages were relevant to the plaintiff's claim and were significant to the resolution of the case); Benebone LLC v. Pet Qwerks, Inc., 2021 U.S. Dist. LEXIS 43449, at *6 (C.D. Cal. Feb. 18, 2021) (finding that Slack messages were relevant because the plaintiff used Slack for part of its internal business communications).

[9] Bad box – A cowboy expression that means "to be caught in a bad situation." https://coloradotrails.com/blog/top-100-cowboy-expressions-and-phrases

[10] https://slack.com/help/articles/203457187-Customize-message-and-file-retention

[11] For more information on the information governance aspects of collaboration technologies, please see our recent webinar titled New Risks of the Evolving Workforce: Information Governance Implications of a Remote Workforce: https://www.ediscoverylaw.com/2022/08/new-risks-of-the-evolving-workforce/.

[12] A recent Slack discovery review project introduced the acronym TL:DR – "too long: didn't read."

K&L Gates is a fully integrated global law firm with lawyers and policy professionals located across five continents. For more information about K&L Gates or its locations, practices, and registrations, visit klgates.com.

RFQ886