

# Draft Commentary on Discovery of Modern Communications and Collaboration Platforms

*The Sedona Conference*

April 2024

Copyright 2024. All rights reserved.



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

## **Draft Commentary on Discovery of Modern Communications and Collaboration Platforms**

### **Drafting Team Members**

Stacey Blaustein	Michelle Briggs
Doug Forrest	Adam Gajadharsingh
Hon. Jane Manning	Benson McGrath
Derek McNally	Jonathan Orent
Jonathan Swerdloff	Cristin Traylor
Beth Wilkins	

### **Team Leaders**

Gareth T. Evans	Joseph P. Guglielmo
-----------------	---------------------

### **Steering Committee Liaisons**

Tara Emory	Meghan Podolny
Maria Salacuse	

DRAFT  
4-10-2024

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

I.	Introduction .....	2
II.	Discussion .....	3
A.	Characteristics of Collaboration Platforms .....	3
B.	Common eDiscovery Issues .....	5
1.	Treatment as Custodial or Noncustodial Data Source.....	5
2.	Preservation Challenges .....	7
3.	Family Relationships and Hyperlinks .....	11
4.	Collection Challenges .....	15
5.	Culling, Search, Review, and Production Challenges .....	18
6.	Evidentiary, Privilege, and Privacy Issues .....	23
C.	Information Governance Considerations.....	27

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

## I. Introduction

This Commentary is intended to provide organizations, lawyers, and the judiciary with foundational information regarding modern communication and collaboration platforms, the technical aspects associated with such platforms, to identify issues and challenges that are likely to arise in eDiscovery, and to provide guidance on how to address them. The use of collaboration platforms has revolutionized the way organizations communicate and collaborate. They enable individuals and groups to work together, to share information, to communicate, and to coordinate tasks seamlessly. They also encompass a wide range of applications, including messaging, document sharing, and video conferencing. Examples at the time of publication of this Commentary include Slack, Microsoft Teams, and Google Workspace.

Although communication and collaboration platforms had been around for years, and their use has steadily grown, the global COVID-19 pandemic of the early 2020s—which caused many workers to work from home—was accompanied by an explosion of their use. By 2021, it was estimated that nearly 80% of workers worldwide used some form of digital collaboration tools.<sup>1</sup> As collaboration platforms have become a primary means of communicating and working, not surprisingly they have also increasingly become a source for discovery. As a source of relevant electronically stored information (“ESI”), however, they can pose conceptual and practical challenges.

The traditional notion of a “custodian”—i.e., someone who has possession and control over ESI—is inapplicable to a group workspace on a collaboration platform, even though members of the group may be performing certain activities that can be associated with a specific custodian (such as messaging, as well as sharing and storing documents). Thus, information created, shared, or maintained on a collaboration platform may not necessarily relate to or be identified with a traditional custodian. This matters because the traditional sense of ESI collection has revolved around the identification and collection of custodial information.

Identifying for preservation purposes relevant shared “groups” on collaboration platforms can present significant challenges. Such shared workspaces can proliferate, and an organization may not possess a comprehensive list of such platforms or their participants to readily identify or assess their relevance to discovery. Complicating matters, “private channels” may exist within a shared workspace and only those who are members may have access to them or be aware of their existence. Additionally, communications and data on collaboration platforms are often stored in various other applications outside of the platform. In Teams, for example, documents and messages are often saved to SharePoint and OneDrive. Thus, careful consideration should be given to identifying information for preservation.

Another unique feature of collaboration platforms is that documents and information are typically shared by means of hyperlinks instead of traditional attachments. Hyperlinked content may be located within the collaboration platform’s environment; it may be located outside the collaboration platform’s environment, but within the organization’s information system; or it may also be located

---

<sup>1</sup> Gartner, Inc. Digital Worker Experience Survey, 2021.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

outside of an organization's information system entirely. As the hyperlinked files are stored in separate locations, and may change over time, finding them and re-associating the correct version to a communication may involve complications that are not present with traditional email and attachments.

These features of collaboration platforms also currently pose challenges for collection and processing in eDiscovery—e.g., locating relevant communications for collection, identifying hyperlinked documents, and associating the correct version of the hyperlinked documents with the contemporaneous message. Collaboration platforms may require different types of culling mechanisms, search strategies, review efforts, and production formats. For example, Considerations may include whether to consolidate communications from a Slack channel into larger units for manageability purposes, such as a 24-hour period, or a particular number of chats. Collaboration platforms may also present unique evidentiary issues. Because collaboration platforms allow multiple users to view and edit a document simultaneously, authentication may be more complex. Additionally, information governance can play a significant role in facilitating organizations being able to fulfill their eDiscovery obligations in the event of litigation or a governmental investigation.

In the sections that follow, we discuss these and many other issues that arise in eDiscovery in connection with collaboration platforms.

## II. Discussion

### A. Characteristics of Collaboration Platforms

A collaboration platform is an application that provides multiple users with the ability to share information and to work collaboratively and often contemporaneously. Collaboration platforms may include the ability to draft, review, edit, and comment on work product simultaneously; to share information, documents, links, files, videos, and audio content; to have live audio and video conferences; and to access recordings and transcripts of the same. The methods of communication in a collaboration platform's environment may include email, chat, video and audio conferencing, wikis, blogs, social media, as well as comments on written work product. Examples of currently available collaboration applications include Microsoft Teams, Slack, Google Workspace, Asana, and Trello. Collaboration platforms may integrate email, text messaging, calendar, and document management tools, and be integrated with existing or legacy stand-alone software. Information created in or accessed through a collaboration platform is not necessarily stored in the platform itself. Rather, the collaboration platform may access and store the data through, or in, another application, so consideration should be given to where the data is stored and how it is accessed.

Modern collaboration platforms generally have the following characteristics that can be used to characterize and understand them:

**Dynamic nature of content:** The documents accessed through a collaboration application are often dynamic and may be changed by multiple users, which may complicate eDiscovery processes such as

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

collection and matching documents with communications in the collaboration application about those documents.

**Not every “document” is a document:** A feature of many collaboration platforms is that the content of a document can be stored in a different format or in multiple discreet parts than what is seen by a user. The content of what appears to be a “document” may in fact be structured data. Data may be stored in a data interchange format such as JSON and rendered in real time for a user. In some instances, the entire history of a document is stored in time-stamped name/value pairs that are rendered viewable by a user in real time by the platform. Each collaboration platform has its own unique schema for storing the data created by the platform.

**The notion of a “custodian” may not apply:** eDiscovery processes often revolve around identifying custodians who are most likely to have information pertinent to a matter and then preserving and collecting relevant information in their possession, custody, or control. While custodians may participate in activities on collaboration platforms, these platforms are—much like a database that a custodian may access—traditionally considered a non-custodial source of information. Thus, consideration should be given when determining how collaboration platforms are accessed and used as the traditional concept of custodial-based ESI does not apply to discovery in many collaboration platforms. Collaboration platforms typically provide shared workspaces and applications that teams or cohorts of users may utilize. Litigants may need to develop eDiscovery strategies for identifying, preserving, and collecting relevant data specific to each tool implemented on or accessed through the collaboration platforms that they use.

**Ability to have conversations within documents:** Collaboration platforms and the applications they incorporate often allow users to make notes and comments within documents, essentially having a conversation within them. Litigants will need to consider and understand how these types of comments will be processed and reviewed. Some platforms may allow extraction and presentation of the data in separate fields, as extracted text, or to show the comments within the document itself. It can be important to understand where this data is stored, viewed, and produced, as that may impact issues such as privilege and confidentiality. If comments are present in the native, but not in the production images, or vice versa, that could cause issues for both the receiving and producing parties. If there is text that needs redaction, producing parties will need to know all the locations where that data resides so it can be redacted properly.

**Hyperlinked documents in lieu of attachments:** Hyperlinked documents are not the same as traditional static attachments but are often used instead of attachments in communications in collaboration applications. Unlike attachments and their parent emails, hyperlinked documents may not be stored directly with their source emails. The documents may reside in applications or sources outside of the collaboration application, but which are integrated into the collaboration platform (e.g., SharePoint Online or OneDrive). They may also reside entirely outside of an organization’s information system, such as on the internet. Because hyperlinked documents are shared and can be updated by one or more users, they may change over time as persons with access revise them. Thus, it is important to understand how the hyperlinked document, and its versions, were maintained

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

because the hyperlink may no longer point to the document as it existed at that time the email was sent or may no longer be available.

**Portals to other applications:** Collaboration platforms may appear to a user as a single, consolidated application providing various features, though they operate as portals to one or more other applications. For example, a team collaborating on drafting a document in a collaboration platform may be working on and storing the document in a separate application that the collaboration platform merely accesses, such as Dropbox or OneDrive. Similarly, instant messages, meeting notes, and calendar entries which appear to a user to be within a platform may be stored within the platform or may, in fact, be stored outside of the platform – whether in a cloud storage location or within a different collaboration platform. Thus, it is important to understand the various features of a collaboration platform and where information from those features may reside.

## **B. Common eDiscovery Issues**

### **1. Treatment as Custodial or Noncustodial Data Source**

Collaboration platforms typically provide shared spaces and embedded applications or functionalities teams or groups of users may utilize. While custodians may access and participate in shared spaces (e.g., “teams” or “channels”) on collaboration platforms, the platforms themselves are usually considered to be non-custodial sources of information. As stated in *The Sedona Principles*, “An organization’s networks or intranet may contain shared areas (such as public folders, discussion databases, and shared network folders) that are not regarded as belonging to any specific employee. Similarly, there may be no one ‘owner’ of the ESI for collaborative workspace areas within the organization.”<sup>2</sup>

Nevertheless, a custodian may individually use—i.e., not as part of a shared space—certain functionalities of a collaboration application. For example, it is common for users to utilize the chat function of some collaboration applications individually, much like an email account. In that circumstance, it may be appropriate to treat a custodian’s chats as a custodial source of information.

Although a custodian’s access to or use of a collaboration platform alone does not necessarily mean that all or a portion of the data in the platform must be preserved or searched, consideration should be given to the use of the platform and the information that may be collected and preserved. This will allow an organization to identify and understand what steps can be taken to preserve, search and produce that information if it is later deemed relevant in discovery. Custodians may be able to assist in identifying the existence of shared spaces in collaboration platforms that are relevant—i.e., those

---

<sup>2</sup> The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 19 Sedona Conf. J. 1, 116 (2018). See also id. at 103 (organizations “should assess the persons likely to have relevant information, and the sources of non-custodial relevant information . . . such as structured systems and databases, and other non-custodial sources such as collaboration tools [and] social media”).



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

involving work product and communications relevant to the issues—because of their involvement in the matters underlying the litigation or investigation.

Understanding how a collaboration platform is being used may be helpful in identifying custodians and other relevant information. For example, most collaboration platforms allow users to collaborate on documents and to communicate in groups or one-on-one (e.g., Teams); some platforms are primarily communication tools (e.g., Discord); while still others are communication and file sharing tools that integrate other cloud-based document management systems (e.g., Slack).<sup>3</sup> Knowing at the outset the capabilities of a given platform will help to determine the scope of potentially relevant information.

Once a relevant shared space within a collaboration platform is identified, it may be possible to identify other users (or collaborators) involved in the underlying matter who may be considered potential custodians or witnesses. Identifying those who actively participated in a relevant shared space can be particularly helpful in the early stages of litigation when the organization is investigating the issues to understand the facts and to determine relevant custodians and sources of relevant information within (or accessed through) the collaboration platform.

Additional potential custodians may be identified by reviewing who collaborated on a project or document, or who communicated in chats and channels, as well as the substance of those communications. Be aware that participants in chats may use pseudonyms (i.e., “handles”) instead of their true names, which may hide or obscure their identities.

Consideration should be given to who had access rights to a group or shared space on the collaboration platform, including whether a specific person was an active or passive participant. For example, an individual could have had the right to make edits to a document but have not made any edits. Likewise, an individual could have been a member of a group chat channel, but not actually have communicated on the channel. Moreover, it is possible an individual may have been given certain access rights without even knowing they were provided. By contrast, if an issue in the case relates to the particular user’s state of mind or knowledge, having even passive access to certain documents or communications may be relevant.

Finally, collaboration platforms often include applications or features that may be used outside of shared spaces. Chats, video calls, and audio calls may be made inside or outside of a shared space, and there may be records related to those calls (such as the date, time, topic, participants, and even an automatically generated transcript or summary of the call). Thus, consideration must be given to those other sources of information, how they are maintained, who maintains custody or control of the information, and whether they can be collected and produced. Understanding the capabilities of a

---

<sup>3</sup> See, e.g., *Hayvin Gaming, LLC v. Workinman Interactive, LLC*, Case # 23-CV-6172-FPG, 2023 WL 3748844, \*2 n.2 (W.D.N.Y. June 1, 2023) (describing Slack as “a collaboration tool that allows teams to message, share files, and archive information”).



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

collaboration platforms and how it is used will be helpful in identifying custodians and discoverable information.<sup>4</sup>

## 2. Preservation Challenges

The principle that litigants have a duty to preserve discoverable information upon the commencement or reasonable anticipation of litigation or a governmental investigation applies to collaboration platforms, just as it applies to other types of ESI. As observed in the *Commentary on Legal Holds*, while the principle “is easy to state,” its “application in practice, however, often requires careful analysis and difficult decisions.”<sup>5</sup> “Nonetheless, each day, organizations must apply the principle to real-world circumstances, first confronting the issue of whether an obligation is triggered, and then determining the scope of their obligation.”<sup>6</sup>

The trigger of the duty to preserve, of course, is no different with respect to collaboration platforms than as to other sources.

Once a duty to preserve is triggered, litigants must take reasonable and proportional steps to preserve ESI that is relevant to the dispute.<sup>7</sup> There is no broad requirement to preserve *all* information.<sup>8</sup> As the *Commentary on Legal Holds* recognizes, “identifying and preserving discoverable information “can be a complex process. It may include creating teams to identify the sources, custodians, and data stewards of discoverable information, to define what needs to be preserved, and to coordinate with outside counsel.”<sup>9</sup> Moreover, personnel with particular knowledge and expertise regarding systems and processes may be needed.<sup>10</sup>

The unique attributes of collaboration platforms should be considered when determining the scope of the duty to preserve, as these platforms may involve a number of complexities associated with the multiple functionalities of these systems and the varying types of information that may be stored and collected. As an initial matter, determine whether an organization uses one or more collaboration platforms and assess the information that the platforms create. Then determine whether the organization and/or the platform vendor maintains the data that is created by the users of the platform

---

<sup>4</sup> See *In re Google Play Store Antitrust Litig.*, 2023 U.S. Dist. LEXIS 53218, \*22 (N.D. Cal. March 28, 2023) (noting that Google Chat’s default retention period for one-on-one chats with “history” turned off is 24 hours).

<sup>5</sup> The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 Sedona Conf. J. 341, 351 (2019) (“*Commentary on Legal Holds*”).

<sup>6</sup> *Id.*

<sup>7</sup> See FED. R. CIV. P. 37(e) (imposing sanctions only if relevant information was lost or destroyed because the party failed to take reasonable steps to preserve it); see also *Commentary on Legal Holds* at 355 (“The proportionality principle applies to all efforts to plan and implement preservation, and in the assessment of those efforts.”) (citing FED. R. CIV. P. 37(e) advisory committee’s note to 2015 amendment (One “factor in evaluating the reasonableness of preservation efforts is proportionality.”)).

<sup>8</sup> *Commentary on Legal Holds* at 356 (citing cases).

<sup>9</sup> *Id.* at 357.

<sup>10</sup> *Id.*

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

and the forms in which such information may be preserved.<sup>11</sup> Although not exhaustive, a good place to start to identify and determine what collaboration platform(s) are used by an organization and if they may possess relevant information is often with in-house counsel, IT personnel who have knowledge of an organization's information systems, and individuals who worked on or were associated with a specific project or program relevant to the litigation.

Additionally, investigating whether there may be relevant information on a collaboration platform may include questions regarding use of the platforms posed in interviews of key employees or in questionnaires sent to potential custodians. These individuals may be asked to identify groups or shared spaces in collaboration platforms that pertain to the events underlying the matter or that are otherwise relevant. Identifying relevant shared spaces or groups may lead to identifying other users with knowledge of relevant facts, who can then be asked if there are other shared spaces or groups that may be relevant to the matter.

Custodian interviews and questionnaires, and discussions with in-house counsel and IT personnel, may not be sufficient alone to identify all relevant sources of information on a collaboration platform. For example, "private channels" may exist within a shared space that those who are not members of the private channel may not even be able to see. It may be helpful to employ other search methodologies, such as searching lists or indices of names of shared spaces (i.e., teams or channels) available to the IT department and sampling the content of spaces whose names appear to be potentially relevant to the issues in the litigation or investigation.

Custodians can also confirm whether they may have used certain features of a collaboration platform either within or outside of a shared space. For example, the chat feature of a collaboration platform may be used in shared spaces, but it also may be used as custodians' primary chat application separate and apart from any group or channel. The chat function on the Microsoft Teams platform, for example, may serve as individuals' primary (or only) work chat application. Accordingly, consideration should be given to whether custodians' chats in a collaboration platform outside of shared spaces should be preserved, much like custodians' email accounts are often put on legal hold.<sup>12</sup>

Once a relevant shared space (e.g., a "team" or "channel") is identified, it is important to determine how and in what form different types of communications and data are stored and can be preserved. Slack, for example, at the time of publication, maintains data as JSON<sup>13</sup> files that identify the user and date-stamped change history of chats and interactions within the platform. The Slack platform itself

---

<sup>11</sup> See, e.g., *FTC v. Am. Future Sys., Inc.*, 2023 U.S. Dist. LEXIS 90014 (E.D. Pa. Mar. 28, 2023) (James J. Rohn, Spec. Master), adopted in part, modified in part by *FTC v. Am. Future Sys., Inc.*, 2023 U.S. Dist. LEXIS 89514, 2023 WL 355319 (E.D. Pa. May 17, 2023) (Joel Slomsky, J.) (Defendant argued that it had no control over its Slack data and that a court order would be required to export Slack data. The special master disagreed and ordered the production of Slack ESI. Although the special master rejected sanctions, he described defendant's failure to produce Slack data, failure to consider Slack as a potential custodian of defendant's data, and failure to even reach out to Slack all "troubling.").

<sup>12</sup> See, e.g., *FTC v. Roomster Corp.*, 2023 U.S. Dist. LEXIS 96290, 2023 WL 4409484 (SDNY June 1, 2023) (Sarah Netburn, M.J.) (after defendant admitted to spoliating Slack evidence despite instituting a legal hold, court permitted plaintiff discovery as to defendant's intent).

<sup>13</sup> <https://www.json.org/json-en.html>

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

is a rendering tool for the stored JSON files, and users do not see the files underlying the platform. Additionally, the collaboration tool may limit the information that can be collected or preserved.<sup>14</sup>

Often, communications and data are stored in various other applications outside of the platform. In Teams, for example, at the time of publication, files uploaded into a channel are stored in a folder in SharePoint. Files uploaded into a one-on-one or group chat are stored in the Microsoft Teams Chat Files in the team's OneDrive for Business folder. Teams meeting recordings may be stored in either OneDrive or SharePoint. It will therefore be necessary to determine whether the files can be preserved in place in the locations where they are kept in the ordinary course of business, or whether they should be collected for preservation purposes. It is also important to recognize that where and how these platforms store data is constantly evolving and changing, so it is necessary to have persons involved in the preservation process who are up to date on the technology.

Some collaboration platforms also contain dynamic documents - the access and control of which can vary by audience and are saved within a database. A user may not see, know, or appreciate the full nature of the documents they are working with. For example, certain users could see all information in a document while others with less extensive permissions could see less. Special tools may be required to preserve the ESI and metadata required to appropriately generate these documents for use in the matter.

Additionally, in communications in collaboration applications, such as chats, it is common for files to be referenced through hyperlinks to other sources, either within or outside of the organization's information system, rather than uploaded to the platform. It can be important, therefore, to consider what may be likely locations of hyperlinked documents, such as a document management system, and whether existing records retention in those locations will be sufficient for preservation purposes.

Indeed, as a general matter, it can be important to be aware of the records retention time periods for data in the various locations where collaboration platform data is stored. Having that information can help guide how quickly targeted preservation measures must be implemented, whether relevant data can be preserved in place, or whether preservation must be effectuated through collection of the data. Thus the retention settings for data on a collaboration platform may be relevant to the discovery being sought.<sup>15</sup>

---

<sup>14</sup> See Commentary on ESI Evidence & Admissibility 22 Sedona Conf. J. 91 at 139-140, n.146-147 (2021) (discussing that a user's ability to export certain information from Slack depends on the specific plan they purchase).

<sup>15</sup> *Drips Holdings, LLC v. Teledrip LLC*, 2022 U.S. Dist. LEXIS 178233, 2022 WL 4545233 (N.D. Ohio Sept. 29, 2022) (John R. Adams, D.J.) (Defendant Teledrip, Inc. used Slack as a usual means of internal and external communication. Teledrip was found to have adjusted the retention settings of the company's Slack environment after learning of potential litigation. In particular, it changed the retention period from un-limited retention to only retaining data for seven days. It also deleted a prior export of Slack data. Teledrip argued that the change, despite the timing, was related to their understanding of the requirements of the California Consumer Privacy Act ("CCPA") and the associated International Standards Organization ("ISO") implementation. The court was not persuaded. Not only had Teledrip altered the retention period and destroyed a prior export, it also refused to update its retention policy to accommodate the legal hold, citing to the CCPA issue. After rejecting the CCPA argument as wrong and characterizing certain

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

Automatic Slack retention settings also led a sanction in *Adler v. McNeil Consultants, LLC*.<sup>16</sup> Defendants in *Adler* used a free Slack subscription that only retained messages for nine days. The defendants made no efforts to preserve any Slack data even after the lawsuit was filed. The court found that possibly relevant ESI was spoliated prejudicing the plaintiff, but the defendants did not intend to spoliolate the Slack data. In fashioning a remedy consistent with defendants' lack of intent, the court's sanction allowed the parties to present evidence to the jury concerning the loss and likely relevance of the Slack messages, and granted an instruction that the jury may consider that evidence in making its decision.

It is possible that some documents that relate to a collaboration platform may be downloaded to a user's account or personal computer, for example where a user works on a "local copy" of a file. Accordingly, a custodian's local hard drive may contain unique copies of relevant information from a collaboration platform.

Further, in seeking to identify relevant ESI within a collaboration platform so that it may be considered for preservation, it is important to understand the collaboration platform's functionalities and the information that it or users may generate.<sup>17</sup> For example, organizations are increasingly using the video and audio features of collaboration platforms for online meetings, and the capabilities of those features are rapidly developing. Depending on the platform and the license level that an organization purchases, it is now possible to obtain a great deal of information about a meeting with a collaboration platform. That information may include a complete recording of the meeting; a list of participants; a record of when participants entered and left the meeting; an artificial intelligence-generated list of action items; an AI-generated transcript or summary of what was said and who said it; identification of documents or hyperlinks shared during the meeting; and a record of all the chat communications connected to the meeting.

Those capabilities are available at the time of writing of this publication and are likely to develop further over time. In the future, there are also likely to be other powerful capabilities that may generate relevant information subject to the duty to preserve. It is important to be aware of the features of each collaboration platform to ensure that the organization has and will take steps to preserve relevant information related to the platform and its use.

---

assertions by the defendants as "blatantly false," the court ordered a mandatory adverse-inference jury instruction as a sanction.)

<sup>16</sup> *Adler v. McNeil Consultants, LLC*, \_\_\_ F.Supp.3d \_\_\_, 2023 U.S. Dist. LEXIS 54771, 2023 WL 2699511 (N.D. Texas Feb. 15, 2023) (David L. Horan, M.J.); but see, *Carty v. Steem Monsters Corp.*, 2022 U.S. Dist. LEXIS 209305, 2022 WL 17083645 (E.D. PA Nov. 18, 2022) (denying sanctions where defendant preserved Discord chat ESI that was subsequently deleted by hacker and where plaintiff could not demonstrate what relevant ESI was deleted as the result of the post-preservation hack.

<sup>17</sup> See, e.g., *Cisco Sys. v. Chung*, 2023 US Dist. LEXIS 48924, at \*15 (ND Cal. Mar. 22, 2023) (Phyllis Hamilton, D.J.) (discussing spoliation of Sharepoint audit logs that would what employees viewed certain documents but declining to impose sanctions).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

### 3. Family Relationships and Hyperlinks

One of the challenges of dealing with collaboration platforms in eDiscovery is that documents and information are normally shared by hyperlinks instead of traditional attachments. With email, traditional attachments are part of a .msg container file along with the parent email. The attachment is usually a static document from a specific point in time. Each email and its attachments are kept together as a “family” and can be readily associated in document collection, review, and production. Collaboration platforms utilizing hyperlinks, by contrast, reference content stored elsewhere, and the referenced content is not transferred with or stored with the message.<sup>18</sup> At the time of publication of this Commentary, traditional email applications are moving away from this paradigm. Cloud-based email, such as email in Microsoft 365 and in Google’s GSuite, may utilize hyperlinks to content rather than attachments stored with the email message in a .msg file.<sup>19</sup>

There are two primary Federal Rules affecting the analysis of relevance as to attachments and hyperlinks. First, Federal Rule of Civil Procedure 26(b)(1) provides that “Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense and proportional to the needs of the case . . . .” Fed. R. Civ. P. 26(b)(1). Second, Federal Rule of Evidence 106, often called “the rule of completeness,” provides: “If a party introduces all or part of a writing or recorded statement, an adverse party may require the introduction, at that time, of any other part — or any other writing or recorded statement — that in fairness ought to be considered at the same time.” Fed. R. Evid. 106. These two rules can result in a tension between what is truly relevant versus what should be produced even if relevance is questionable, in order to provide the context of the communication.

Hyperlinked content may be located within the collaboration platform’s environment, such as in SharePoint or OneDrive in the Microsoft Teams environment. It may be located outside the collaboration platform’s environment, but within the organization’s information system such as a document administration system like iManage. Hyperlinked content may also be located outside of an organization’s information system entirely, such as hyperlinked content on a website. As the hyperlinked files are stored in separate locations and may change over time (including no longer being present in the target location, i.e., a “broken link”), finding them and re-associating the correct version to a communication may involve considerations and complications that are not present with traditional

---

<sup>18</sup> Various terms have been proposed for hyperlinks and the content to which hyperlinks point. “Pointers” and “modern attachments” are two examples, respectively, and they have engendered a fair amount of controversy. This Commentary uses the term “hyperlinks,” as that term is defined in The Sedona Glossary (“Hyperlink: A pointer in a hypertext document—usually appearing as an underlined or highlighted word or picture—that, upon selection, sends a user to another location either within the current document or to another location accessible on the network or internet.”). This Commentary also uses the terms “hyperlinked documents” (or files) and “referenced documents” (or files) for the documents or files to which the hyperlinks direct.

<sup>19</sup> See, e.g., *Shenwick v. Twitter*, No. 16-CV-05314 (JST)(SK), 2018 U.S. Dist. LEXIS 189263, at \*1 (N.D. Cal. Sept. 17, 2018) (observing that emails in GSuite use hyperlinks to reference documents stored in the GSuite environment, “and sender and recipient can then modify the referenced document, which is stored centrally so that more than one person can access it.”).



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

email and attachments. Accordingly, traditional notions of document “families” may not necessarily apply.

Not all hyperlinked content will be relevant to the issues. Thus, requests for “all” hyperlinked content should be viewed skeptically. An organization cannot avoid production of relevant information, however, simply because it utilizes hyperlinks to share content. Accordingly, determining the relevancy and responsiveness of hyperlinked content is no different than with traditional documents. The need to consider relevance, burden and proportionality is unchanged because information is shared by hyperlinks. Parties should discuss and consider the scope of production of hyperlinked content. For example, hyperlinks can point to specific documents stored in a collaboration platform’s environment. By contrast, a hyperlink may not point a specific document; rather, it could point to an entire folder containing hundreds of files, only some of which are relevant.

A particularly problematic issue related to the identification and preservation of links is versioning, which is when an electronic record changes in some way to create a new version of it. These changes can include modifications to file format, metadata, or content. Collaboration platforms and the use of hyperlinks can result in a linked document that has undergone numerous changes or edits from the time the hyperlink was originally used in an email to when ESI is being preserved or collected for a case. Certain collaboration platforms may automatically save each version of document, while other collaboration platforms may not. For document administration systems like iManage, retaining versions of collaboration documents is an essential function in order to track stakeholder participation in the editing of the document. Beyond these functional capabilities, in a litigation context, the ability to capturing all versions or a specific version could be critical to a specific situation.

Understanding the capabilities and potential limitations of a collaboration platform can help evaluate potential burden issues for the producing party. In addition, for “active” documents undergoing changes, matching the version at the time of the email can be difficult or impossible to resolve depending on how the data is stored. Furthermore, it may not even be possible to identify the version of a document as it existed at the time the hyperlink was first used because such information was not preserved in the normal course or that version may have been deleted prior to when a party’s duty to preserve was triggered. Thus, one of the very reasons organizations utilize hyperlinks, to foster collaboration on documents, also presents one of the greatest challenges in discovery.

eDiscovery and records retention demands have driven the evolution of functionalities to help address these issues. The licensing level an organization purchases frequently dictates the extent to which helpful solutions are available. Thus, an organization should understand the capabilities and level of access available when utilizing a collaboration platform. For example, the “Standard” license of early versions of Microsoft 365, which can include Teams, did not provide any ability to automatically preserve the “as-sent” versions of hyperlinked documents, nor to identify or preserve hyperlinked content even in locations within the Teams environment, such as SharePoint or OneDrive.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

An early “Premium” license for Microsoft 365 may provide more functionality but may not have all of the capabilities one may need for eDiscovery purposes. For example, upon implementation of a legal hold, it would associate the most recent version of a hyperlinked document with the message containing the hyperlink. It would also facilitate identifying and putting on hold sources within the Microsoft 365 environment such as OneDrive and SharePoint.

Nevertheless, with either license, an organization would have needed to choose among various imperfect preservation strategies involving risks of either over-preservation or under-preservation, such as preserving the entire storage source where the hyperlinked document is stored (e.g., SharePoint or OneDrive), or to use date ranges, search terms, or other methods to preserve a subset of documents stored in those sources. For review and production purposes, the organization might be faced with the task of manually trying to align a “close to” as-sent version of the hyperlinked document—possibly a burdensome and resource-intensive process. An open dialogue with the requesting party can avoid overcollection as in many cases they have no need for the drive pointed to by a hyperlink and will work to make sure that productions are tailored towards only responsive material.

More recent versions of the software address some of these problems. A feature was added for Premium subscribers that allows organizations to retain a copy of the as-sent version of a hyperlinked document (within the Microsoft 365 environment) at the time it was sent. The system would then treat this copy of the hyperlinked document and the message containing the hyperlink as a “family.” This feature would need to be set in advance as a retention policy before the message with the hyperlink was sent and could not be implemented retroactively. Indexing of versions of documents in a source within the environment may also facilitate searching for the as-sent version of a hyperlinked document, but doing so could still be a burdensome process.

Similarly, software providers have been developing tools that can collect and associate some, but not all, hyperlinked documents with messages containing the hyperlinks. One example is a computer forensics software which claims to automatically detect and acquire hyperlinked Google Drive documents during Gmail and Google Workspace collections, presenting them in a package that maintains relationship between the email and hyperlinked document. Another application claims to identify and collect hyperlinked documents from wherever they may exist in the SharePoint or OneDrive environments and to associate them with Teams messages containing the hyperlinks. The tool also compares the communication date of the Teams message to the version history of each file to associate the version shared at that point in time. Regardless of the tool, in order for an organization to adapt to preserving, collection and production of hyperlinks, it will require coordination with IT to ensure that the suitable tools, with suitable licenses, are in place. The collection, review and production of hyperlinked documents will be predicated on detailed and tracked workflows that can capture these documents while retaining the clean and accurate metadata required for production.

As the use of hyperlinks continues to grow, additional tools will be developed to address the challenges associated with discovery of hyperlinked documents. The tools described above that exist as of the time of publication of this Commentary, however, have significant limitations in that they are only



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

able to associate hyperlinks in collaboration platform messages with hyperlinked documents in the collaboration application's environment. They are not able to make these associations where the hyperlinked content is outside of the collaboration platform's environment, e.g., Microsoft 365 email with Google Drive links or Google Mail links to OneDrive or SharePoint. They also may not be able to collect hyperlinked content retroactively -- they must be used at the time of collection. In addition to being knowledgeable about the availability and functionalities of tools to address these issues, organizations will also need to be cognizant of the costs involved. Indeed, organizations may be well served by considering these issues in configuring their information systems and in their information governance, so as to avoid complex and expensive problems in fulfilling eDiscovery obligations when litigation comes.

In light of the technical challenges and burdens involved, as soon as the initial meet and confer, litigants may exchange information sufficient to understand the technical capabilities of how hyperlinks are associated with a collaboration platform. This can allow the parties to have an informed discussion regarding the scope of production of hyperlinked documents and the burdens associated with producing relevant hyperlinked information.

Although certain attachments may not be relevant on their face, there often is a presumption they are relevant because they were intended to be included for a substantive reason and, therefore, are likely to provide helpful context regarding the parent. This presumption carries less weight if applied indiscriminately to all hyperlinked documents because, as discussed below, not all hyperlink documents are the same and may not be a necessary part of the overall communication. The better practice is to request only those hyperlinks that are likely to be relevant.

Hyperlinked content also may not even have been intended to be a necessary part of the communication containing the hyperlink. The court in *Nichols v. Noom*, for example, stated that “[a] document might have a hyperlink shortcut to a SharePoint folder. The whole folder would not be an attachment.”<sup>20</sup> Similarly, “[a]n email might have hyperlinks to a phone number, a tracking site for tracking a mailing/shipment, a Facebook page, a terms of use document, a legal disclaimer, etc. The list goes on and on.”<sup>21</sup>

In *Nichols*, plaintiffs sought to compel defendant to reproduce hyperlinked documents with associations to specific emails. The court held that it did “not agree that a hyperlinked document is an attachment[.]”<sup>22</sup> Based on a proportionality analysis, the court ruled that defendant did not need to reproduce hyperlinked documents that were previously produced separately and associate them with emails containing hyperlinks.<sup>23</sup> Nevertheless, the court also ruled that plaintiffs could request “an additional targeted pull or production or clarifying information about a hyperlinked document’s identity or Bates number.”<sup>24</sup>

---

<sup>20</sup> *Nichols v. Noom Inc.*, 20-CV-3677 (LGS) (KHP), 2021 WL 948646, \*4 (S.D.N.Y. March 11, 2021).

<sup>21</sup> *Id.*

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

As in *Nichols*, other courts in considering motions to compel the production of hyperlinked documents along with the messages containing associated hyperlinks have assessed the relative burdens and proportionality factors, and have crafted orders accordingly. *Shenwick v. Twitter, Inc.*, for example, involved a motion to compel production of 725 hyperlinked G Suite documents along with the emails containing associated hyperlinks.<sup>25</sup> The defendants objected because they had already separately produced the G Suite documents, and they argued that it was burdensome to re-associate the documents with emails containing the associated hyperlinks. The court granted the motion to compel, but limited plaintiffs to 200 messages with hyperlinks and their hyperlinked documents.<sup>26</sup>

Similarly, in *Iqvia, Inc. v. Veeva Systems, Inc.*, the plaintiffs moved to compel 2,200 hyperlinked Google Drive documents.<sup>27</sup> The defendant agreed to separately produce hyperlinked documents, but argued that re-associating them with emails was unduly burdensome. The special master, in granting the motion to compel however, was “not convinced” that re-associating the documents was disproportionate in light of proportionality factors. By contrast, in *Porter v. Equinox Holdings, Inc.*, the plaintiffs sought to compel the defendant to produce all hyperlinked documents with associations to the specific family emails containing the respective hyperlinks.<sup>28</sup> The court denied plaintiffs’ request. Instead, the court followed the approach of *Nichols v. Noom*, holding that plaintiffs could make reasonable requests for targeted, important documents to be produced with association to emails containing hyperlinks.

There are no bright line rules from statutes or case law governing the production of hyperlinked documents other than that requests for “all” hyperlinked content is generally too broad and claiming that any production of hyperlinked content at all is too burdensome is a nonstarter. Utilizing meet and confers and other methods to create a measured dialogue between parties about the nature of their respective data and the proper steps to pinpoint a search for relevant hyperlinked documents appears to reflect the core of our traditional approach to locating relevant documents. A robust understanding and communication of the policies, protocols, and tools in place for preserving, collecting, processing, reviewing, and producing relevant hyperlinked documents can be helpful for counsel to resolve issues of burden and proportionality.

#### 4. Collection Challenges

Collaboration platforms may present a number of collection challenges for purposes of eDiscovery. One of the primary issues is that some collaboration platform communications and documents may not be stored with the collaboration platform itself, but rather with other applications both within its immediate environment – e.g., certain types of communications and files in Microsoft Teams stored in SharePoint or OneDrive – and without – e.g., communications in Slack with links to files in Google

---

<sup>25</sup> *Shenwick v. Twitter*, 2018 U.S. Dist. LEXIS 189263, at \*1.

<sup>26</sup> *Id.*

<sup>27</sup> *Iqvia, Inc. v. Veeva Systems, Inc.*, Case No. 2-17-cv-00177-CCC-MF 2019 WL 3069203 at \*5 (D.N.J. July 11, 2019)

<sup>28</sup> *Porter v. Equinox Holdings, Inc.*, Case No. RG19009052, 2022 WL 887242, at \*2 (Cal. Super. Mar. 17, 2022) (“[L]inked documents can present unique challenges that make them different from email attachments.”).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

Drive or Box. Accordingly, it is important to understand where relevant and responsive information is likely to be located in order to collect it.

Documents and files are normally shared in collaboration platform communications by means of hyperlinks rather than files stored within the collaboration platform itself. Depending on the capabilities of the collaboration platform and, sometimes, the level of license purchased, it may be possible to find and collect the hyperlinked content in applications that are in the collaboration platform's environment (e.g., SharePoint and OneDrive in the Teams environment). Software tools may also be available to associate and collect hyperlinked documents with the messages referencing them, and to present them in a form analogous to a traditional document "family," though at the time of publication this functionality was generally limited to applications operating on data within the collaboration platform's environment.

Where such capability is not available, for example in some instances where hyperlinks reference content outside of the collaboration platform's environment, responding parties will need to consider other approaches to finding and collecting hyperlinked content and the burdens associated with such approaches. For example, they may need to conduct a less targeted collection from the source where the hyperlinked content is located and then to conduct searches to associate the correct hyperlinked document with the message containing the hyperlink.

Doing so can be further complicated if there could be multiple versions of the hyperlinked document, which may require employing manual or automated processes to find the version of the hyperlinked document that existed at the time of the message referencing it. An exact match with the hyperlinked document as it existed at the time of the message may no longer exist due to revisions subsequently made to the document. Nevertheless, some linked documents—e.g., pdf files or images—may either be effectively immutable or unlikely to be revised. Thus, collecting the correct hyperlinked document or the correct version of the hyperlinked document can be complicated and may require programming or manual review, which could be more expensive than if commercial software to address the issue were widely available at a reasonable cost.

With respect to collecting data from the collaboration platform itself, the best practice is usually to engage a data collection professional with expertise in collecting data for litigation purposes. Such professionals may be found either within an organization's information technology department or through external providers. They should have knowledge of the options available for collection, including the functionalities available in the collaboration platform application and other software tools available to collect data associated with collaboration applications.

Nevertheless, it can be helpful for counsel to understand collection options and the extent to which there are limitations associated with them. One option, perhaps the most basic, is collecting data through download functionality in the platform itself. Known as "DYL" (download your

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

information)<sup>29</sup>, these tools usually limit the scope, and accordingly volume, of information that can be extracted from the platform. Therefore, it is important to understand what these limitations are before relying on this technique for eDiscovery collection purposes.

Additionally, DYI downloads may not be directly loadable into an eDiscovery review platform or be in a format that can be readily ingested by an eDiscovery processing program.<sup>30</sup> Commercial software tools exist, however, that can process some DYI downloads into RSMF (Relativity Short Message Format) or review platform-ready load files.

Data can also be extracted from a collaboration platform through the platform's API (application programming interface). API's are interfaces for programs and programmers to access a platform programmatically. For example, Google provides an API to enable its clients and commercial software developers to interface directly with Google drive documents and folders by creating programs that retrieve files in Google Drive.<sup>31</sup> Similarly, Microsoft provides an API to retrieve SharePoint documents using Microsoft's SharePoint REST API.<sup>32</sup> Commercially available tools and those used by eDiscovery service providers may use multiple APIs from different platforms to address some heterogeneous environments, for example to collect Slack threads and messages and then to collect the hyperlinked documents to those messages resident on Google Drive. There may not be commercial programs that can collect all of the information together or in an associated fashion, however, for other heterogenous environments—perhaps, for example, using Microsoft Teams but storing linked attachments outside of the Teams environment.

API's, moreover, can present challenges in data collection. As stated in the *The Sedona Commentary on ESI Evidence and Admissibility*, “[a]n API collection lacks perfect synchronicity with the original content—it may change its context, format, or appearance—and it may be difficult to access. Moreover, provider restrictions may limit the amount of data that can be collected through an API.”<sup>33</sup>

Finally, the ability to collect collaboration platform data may depend on the type of license or subscription the producing party has for the platform. For example, the Enterprise version of Slack

---

<sup>29</sup> See <https://www.facebook.com/help/212802592074644>; <https://help.snapchat.com/hc/en-us/articles/7012305371156-How-do-I-download-my-data-from-Snapchat>

<sup>30</sup> For example, Facebook DYI downloads come in HTML or JSON format.

<sup>31</sup> See, e.g., Introduction to Google Drive API, available at <https://developers.google.com/drive/api/v3/about-sdk> (accessed on June 5, 2023).

<sup>32</sup> See, e.g., *Get to know the SharePoint REST service*, available at <https://learn.microsoft.com/en-us/sharepoint/dev/sp-add-ins/get-to-know-the-sharepoint-rest-service> (accessed on June 4, 2023).

<sup>33</sup> The Sedona Conference, *Commentary on ESI Evidence and Admissibility*, 22 SEDONA CONF. J. 139-140 (2021).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

has more options for preservation and collection than the free version. Microsoft's Purview eDiscovery Premium (E5 license) has more advanced functionality than its Standard (E3) offering.<sup>34</sup>

## **5. Culling, Search, Review, and Production Challenges**

### **a. Culling**

Once collaboration platform data is collected, parties must decide whether additional culling should occur prior to search, review, and production. Additionally, decisions may need to be made at the processing stage that will affect the form in which the data is reviewed and produced. For example, document unitization—e.g., dividing continuous communication strings such as chat or instant messages into more manageable units, such as a 24-hour period—may need to take place at the processing stage. Different types of documents and communications on collaboration applications also may involve different types of culling, search, review, and production issues.

Culling collaboration platform data may involve examining the data for content, context, metadata, and other attributes, and applying various techniques to filter, categorize, and prioritize the data. For example, some common techniques for initial culling of chat and instant message data are deduplication, deNISTing, keyword search, date range, concept search, and near-duplicate detection.

Deduplication is an additional culling issue that should be considered. For chat and instant messages, decide whether they will be deduplicated across custodians or whether there is value in producing the same messages multiple times. If deduplication is preferred, verify that the tools used can perform this type of deduplication. For collaboration documents, determine whether every version of a document may be relevant to the claims or defenses, or whether the production can be limited in some way. Collaboration tools may store each modification as a separate version, resulting in thousands of versions, many of which may have only immaterial differences.

For chat and instant message data, consider whether the collection should be limited to certain date ranges. Unitizing (i.e., breaking up) continuous message strings into smaller pieces is becoming a common practice. Options include breaking up strings into 24-hour daily periods or into a certain number of messages. If all of the relevant participants are in the same time zone, it may be best to process in that local time zone and unitize at Midnight of every 24-hour period. If the participants are located in different time zones, then processing in UTC and unitizing either by 24-hour periods or by breaks in discussion may be preferred. Another potential solution may be organizing the collection by subject matter, although you can still have issues where related conversations span multiple days. At the time of the publication of this Commentary, Microsoft's Purview Premium, for example, creates "transcript" files in 24-hour windows. Messages can be converted to Relativity's Short Message

---

<sup>34</sup> *In Calendar Research LLC v. Stubhub Inc.*, 2019 U.S. Dist. LEXIS 65307 (2019), for example, the plain-tiff requested Slack messages from an individual defendant's employer. Because the employer had a free Slack account, certain Slack folders were not retrievable. The defendants paid for an upgraded account, but Slack denied full access because not all the parties on the account had consented. Slack provided a "utility tool," however, to target the channels used by the individual defendants.



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

Format (RSMF) in 24-hour or other time periods for review and production. There are also other technologies on the market that will allow parties to create other groupings of messages.

Consider how comments within documents will be treated during review and production. Determine whether comments can be extracted during processing and loaded to a metadata field. Also, determine whether an eDiscovery review platform will show the comments in the viewer and extracted text, and when the documents are tiffed whether the comments will show on the image. The answers to these questions will determine what can be done with them from a production standpoint. Producing parties should set expectations of how these will be handled during the review and production process. If the comments can be reviewed and produced, then they should be to the extent they are not privileged or otherwise protected from disclosure.

#### **b. Search and Review**

Common search methodologies in eDiscovery include using keyword searches (also referred to as “search terms”) and using technology-assisted review (TAR), such as various types of supervised machine learning, a form of artificial intelligence (AI). At the time of this publication, the legal technology industry is in the early stages of developing large language-model (LLM) Generative AI-based tools for potential use in search and review. AI may also be able to assist in grouping topically related chat and instant messages together (“smart grouping”), which may be the preferred way to review.

Despite the availability of TAR and other AI methodologies, keyword searches are still commonly used for search and review. Producing parties should carefully consider whether search terms are a viable option for chat and instant messages. If used, search terms should be tailored to the nature of both chat and instant messages in general and the specifics of the matter, but flexible enough to collect communications where abbreviations are commonly used and misspellings can occur. Thus, it is necessary to understand what abbreviations, acronyms, shorthand, and slang are likely to be used by the communicants in the specific matter. Doing so can also be important for identifying privileged communications, as attorneys may just be referred to by an abbreviation or a nickname in chat and instant messages. Once the data is collected, producing parties can analyze samples to get an understanding of how users are communicating within these platforms.

In analyzing the data, pay special attention to the use of emojis and GIFs. Depending on the nature of the matter, these may be important to decoding the communications. Verify what capabilities the platform has for searching and analyzing emojis and GIFs, and apply them accordingly.

Part of the analysis can also include evaluating whether different terms may be necessary for the chat and instant message data compared to emails and other forms of ESI. Users often communicate much more informally on collaboration platforms than they do in emails, for example. Therefore, the same search terms may not yield the intended results. As with all searches, the efficacy of keyword searches may be tested by running proposed search terms and sample the hits and non-hits to look for additional terms, and to determine whether search terms may or may not be appropriate in the matter.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

It can be important for the ESI protocol in the case to contain provisions that allow for such an iterative approach, with analysis and sampling, and parties should not agree to specific search terms prior to testing them.

The following are practice tips for using search terms on chat and instant messages:

- Use search terms that are specific and relevant to the issues in the case, and avoid using terms that are too broad, vague, or common.
- Use search terms that are incorporate abbreviations and commonly used terms consistent with the language and terminology used by the parties, witnesses, and custodians in the chat and instant messages, and avoid using terms that are too technical, legal, or formal.
- Use search terms that are inclusive and comprehensive of the variations and synonyms of the key terms, and avoid using terms that are too narrow, literal, or exact.
- Use search terms that are compatible and appropriate for the format and structure of the chat and instant messages and avoid using terms that are incompatible or inappropriate for the data type, metadata, or content.
- Use search terms that are validated and tested for accuracy and effectiveness.

TAR and other AI-based tools may also be used for search and review of collaboration platform data, although parties should carefully consider whether the model is providing reasonable results. Potential issues include there not being enough text in chat and instant messages for machine learning to accurately identify them as likely to be responsive or not.

### **c. Production**

#### **i. Content of Production**

When it comes to determining what information from a collaboration platform should be produced, a number of considerations must be given. Parties should discuss and attempt to agree upon the content of production in an ESI protocol to avoid potential disputes. For example, as discussed above, there is no clear definition of “family” when it comes to chat and instant messages; thus communications can be “standalone”, or they can be part of a related conversation. The concept of what is associated with a document or what a document “family” may include the message plus any hyperlinked content or reaction (e.g., a Gif or emoji) that is part of the individual message, or it may be the entire conversation across multiple days. Consideration of what constitutes a single communication or a family is not clearly analogous to an email and attachment where each message can be analyzed and relevance determined.

Producing parties reviewing chat messages on collaboration platforms may need certain context to determine relevance. Some proposed methods to identify responsive messages may include an agreement that a certain number of messages before and after a responsive chat message be produced, or communications from a specific time period or date range. The potential downsides to this approach include that there may be messages outside the selected message range that would also provide helpful context, and those messages would not be produced if the parties are following the



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

protocol. However, nonrelevant messages that may be produced, which could contain personal and sensitive information. Communication within chat and instant messages may jump from one subject to another in quick succession, and then back to earlier subjects.

Depending on the parameters of the review and the platform, parties may either redact the privileged messages, or create separate “slices” of the privileged and non-privileged messages. Some platforms allow users to code at the message level and/or allow users to select messages that are responsive and create a separate record (or “slice”) for production. Users can also select messages that are privileged and create a separate record (or “slice”) for logging purposes. Identifying privilege may be more complicated when dealing with chat and instant messages. Attorneys may be referred to as first names only or as initials, or some other shorthand, which will be easy for reviewers to miss. Another complication is that people may be communicating with an attorney by email, but then jump platforms to Slack or Teams and start discussing the legal advice provided in the email, but not include the attorney in the chat or instant message communication. It may be difficult for reviewers to recognize that privileged content without the benefit of the context of the other platforms. Parties should keep in mind that reasonableness is the standard and not perfection. If cross-platform communications are later determined to be privileged from context not apparent from standalone review, parties should allow leniency for clawbacks.

## **ii. Form of Production**

Parties should discuss and memorialize the form of production from collaboration platforms in their ESI protocol, just like they would with other discovery requests. Note that this may also be technology dependent and may change as the technology advances. Standard tiffs/pdfs, plus text, metadata and load files should be sufficient for chat and instant messages. There currently is no “native format” production option for chat and instant messages. In the future, parties may be able to exchange production in RSMF so that they can review it in a way that simulates the native application. Other collaboration platforms may be able to be produced in native format, if needed. Parties should evaluate the technological options, keeping in mind how the data will be used in depositions and at trial. A static format may be preferred for ease of use.

Parties should discuss what metadata should be produced from chat and instant messages. For example, if parties are reviewing in 24-hour daily periods, they may only have the metadata from the first message of that day, or they may be able to provide metadata for all the individual messages. Or they may be able to provide all the participants and a date range, but not an entry for each message. It is important to understand the technical limitations prior to agreeing to a format that is not readily available. Parties should discuss what metadata is readily available and also discuss any burdens associated with production of such information.

If individual messages are produced as separate records, parties should produce a field to indicate family relationships (messages and attachments). If possible, parties should produce a field that indicates context groups.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

If reviewing and producing multiple messages together as one pdf or tif, they may redact individual privilege messages. If creating slices, the parties may agree to produce a privileged placeholder for the slice of messages that was withheld (in addition to any logging that is negotiated). Parties should discuss treatment of unavailable/unproduced attachments. These might either be by image placeholders or withheld (non-responsive attachments).

Collaboration and communication platform data must be produced in a way that is useable. It is axiomatic that disclosed information is useful to the opposing party only when it can be organized and accessed logically. A producing party may be tempted to release large amounts of data and place the burden on the requesting party to find what they requested. Even if the producing party is not purposefully “hiding a needle in a haystack,” document dumps are disfavored by the courts. Further, parties should consider what value information may be garnered from *how* collaborative platforms are used, independent of the communications and documents contained therein, particularly with respect to how individuals or documents are organized within the platform and be prepared to request or produce documents in a way that preserves this information.

In *Gopher Media v. Spain*, 2020 U.S. Dist. LEXIS 260540 (S.D. Cal. Aug. 24, 2020), the plaintiff produced Slack messages in response to the defendants’ requests for production. The defendants could not open the file and subsequently complained that the messages were not Bates-numbered. The plaintiff then produced over 139,000 Slack messages as individual documents. The plaintiff did not provide any reference as to which messages responded to which request for production. The plaintiff merely supplied a generic response to each request: “documents already produced in this case.” The defendants complained that many of the produced Slack messages were not relevant “to the action at all.”

The U.S. District Court for the Southern District of California ruled that the plaintiff needed to amend its responses “to identify which documents are responsive to which requests.” Noting that discovery rules prohibit production of “a mass of undifferentiated documents for the responding party to inspect,” the court ruled that the 139,000 individual-documents-dump did not constitute a “reasonably usable format” within the meaning of FRCP 34(b)(2)E(ii). According to the court, the document dump effectively shifted the burden of review for responsiveness from the plaintiff to the defendants.

In *Podium Corp. v. Chekkit Geolocation Servs.*, 2022 U.S. Dist. LEXIS 98197 (2022), the U.S. District Court for the District of Utah, Central Division analyzed a discovery dispute similarly to the court in *Gopher Media v. Spain*. The plaintiff argued that it produced the documents, including Slack messages, “as they are kept in the ordinary course of business.” That may be, said the court, but discovery rules exist to “facilitate the production of records in a useful manner to minimize discovery costs.” The court ruled the production of documents must be organized in such a way that the requesting party may determine with reasonable effort which documents are responsive to its requests.” Noting “wholesale dumping of documents” does not satisfy a producing party’s obligations when responding to interrogatories or requests for production, the court compelled the plaintiff to Bates-number the documents and identify which documents were responsive to particular requests for production.

In contrast to judicial concerns about dumping documents and flooding the opposing party with too much information, some courts found that the responding parties did not provide enough information

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

in their discovery disclosures. Information contained in continuous message streams may need context and even irrelevant, nonprivileged communications must be disclosed to provide such context. In *Bidprime, LLC v. Smartprocure, Inc.*, 2018 U.S. Dist. LEXIS 222868 (2018), the U.S. District Court for the Western District of Texas, Austin Division ruled that the responding party is not within its rights to redact irrelevant information and full chat logs must be produced. In *Lubrizol Corp. v. IBM Corp.*, (get cite), the U.S. District Court in the Northern District Ohio, Eastern Division found that production of entire Slack threads containing only one responsive message overly burdensome. It ruled that, if the Slack conversation has fewer than twenty messages, the entire channel must be produced. Again, context is key. If the channel has more than twenty messages, the ten prior messages and ten subsequent messages must be produced.

Collaboration platforms may store files in ways that have their own value as compilations, independent of whether documents contained therein are duplicative of custodial productions. In securities litigation involving Pfizer, it was discovered that Pfizer used a platform called “eRooms,” a collaborative application for employees to share documents, conduct discussions/instant message, and conduct informal polls. *In re Pfizer Inc. Securities Litigation*, 288 F.R.D. 297 (S.D.N.Y. 2013). The court recognized that “[a]lthough the eRooms contain documents that may be largely duplicative of the custodial productions, they have a value in of themselves as compilations. The manner in which Pfizer and its employees internally organized documents is relevant because it allows Plaintiffs to draw connections and understand the narrative of events in a way not necessarily afforded by a custodial production.” *Id.* at 317.

## **6. Evidentiary, Privilege, and Privacy Issues**

Documents and communications exchanged and stored on collaboration platforms present evidentiary and privacy issues, often without analogues to traditional ESI.

When word processing documents are shared and simultaneously edited by multiple employees in a workspace that overwrites the document with every edit, issues affecting admissibility may arise. For example, the author or custodian of a document may be difficult to identify, making resolution of authentication and hearsay challenges trickier. If multiple people work on a document, who should be the person to authenticate or lay a foundation to overcome hearsay issues? If a document is shared with recipients by hyperlink in an email or chat communication, is the version of the document produced in litigation the same version that was shared? Consideration also should be given to privilege and privacy issues. For example, when multiple individuals in different jurisdictions are working on a document, which jurisdiction’s privilege or privacy laws apply?

Parties should consider and discuss early in the process evidentiary and privacy issues that may arise from the discovery of information from collaboration platforms.<sup>35</sup>

### **a. Evidentiary Concerns**

---

<sup>35</sup> *The Sedona Conference, Commentary on ESI Evidence & Admissibility*, Second Edition, 22 Sedona Conf. J. 83 (2021) 173-174, 179 (parties should consider ESI evidentiary issues early in the case and ensure they have defensible preservation and collection protocols).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

(1) *Authenticity*

Collaboration platforms may present unique issues pertaining to the authenticity of a document. *See* Fed. R. Evid. 901(b)(1). Given that collaboration platforms allow multiple users to view and edit a document simultaneously, authentication may be more complex. *See* Sedona Conference Journal, Vol. 22, at 156 (2021). It may be necessary to rely upon other evidentiary rules to authenticate documents from a collaboration platform, such as \_\_\_\_\_. *See* Sedona Conference Journal, Vol. 22, at 139-140 (discussing collaboration tools and the various ways to authenticate them), 194-209, 218 (identifying methods of authentication for various types of evidence and providing supporting case citations). One other avenue is to consider is whether documents from collaboration platforms can be authenticated by a qualified person pursuant to Fed. R. Evid. 902(14). *See also*, Sedona Conference Journal, Vol. 22, at 98-104 (discussing the two new subsections to Rule 902 and their application), 156-168 (discussing digital identification methods). *See also* Sedona Conference Journal, Vol. 22, at 149-151 (2021) (discussing the challenges of Rule 902(14)).

(2) *Hearsay*

As with authentication, testimony often lays the foundation for a hearsay exception—for example, that an out-of-court statement is a statement by a party opponent or that it meets the criteria for a business record. *See generally* Fed. R. Evid. 803. Where multiple people are collaborating on a document, however, identifying the author of the statement may be difficult, making it challenging to comply with Rules 801(d)(2) (statement of an opposing party is not hearsay) or Rule 803(6) (requiring statement of a custodian to establish hearsay exception for records of a regularly conducted activity by a business or organization). Additionally, employees may use chat platforms, like Slack, to discuss mixed business and personal matters raising questions as to whether specific chat records are properly considered to be business records. Furthermore, such chat platforms may be used by employees but are not officially sanctioned by the organization for use. Thus, identifying the use of a collaboration platform is necessary to understand how the information may be admissible as a business record.

To the extent that a Rule 902 certification is being used, a producing party might consider whether it can include language to lay the foundation for business records. *See* Sedona Conference Journal, Vol. 22, at 167 (2021) (proposing a certification that includes the requirements to satisfy both the authentication and hearsay rules). Where it is difficult to establish that either Rule 801(d)(2) or Rule 803(6) applies, one might consider whether Rule 807 (hearsay exception where the statement is supported by sufficient guarantees of trustworthiness under the totality of the circumstances) could apply. *See id.* at 152-155 (discussing the changes to Rule 807).

**b. Privilege and Work Product Concerns**

(1) *Work Product Doctrine*

Sometimes, collaboration platforms may not specifically maintain records of the author, recipients, participants or contributors of information, which may complicate the analysis of determining whether the work product doctrine applies. With traditional documents, identification of work product was

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

more likely to be straightforward. A memorandum prepared in anticipation of litigation or for trial by counsel providing legal advice is often recognizable for what it is. In the context of collaboration platforms, traditional examples of work product may be the exception rather than the rule. Communications are often more informal, such that it may not be apparent whether content or materials have been gathered or prepared by a non-lawyer at an attorney's direction. Establishing a clear record at the front end that information is work product and limiting access to the communication from its initial inception forward can save time when reviewing information for discovery, and prevent the inadvertent waiver of the work product protection.

## *(2) Attorney-Client Privilege*

Attorney-client privilege may apply if the confidential communication is made for the purpose of legal advice. Accordingly, understanding the context is vitally important. Collaboration tools like Slack, however, often involve a long stream of different conversations over time, which can make separating out the portion of the conversations regarding discrete subjects (and which may invoke attorney-client communication protection) more difficult. Further complicating matters, ongoing chats might stray into less formal conversations and, as such, may contain mixed-purpose communications in one long chain of text. This can make it more difficult to identify the context of the communication, whether the primary purpose of the communication is for legal advice and whether the legal advice can be separated from the remainder of the communication.

When attorney-client communications are made using a collaboration platform, consideration should be given to identifying the communication as seeking or providing legal advice, and to limiting permission rights and access to such communications so as to avoid waiver. Taking steps at or prior to the time of the communication such as explicitly identifying the communication as one with an attorney, seeking legal advice, or relating to anticipated litigation can help ensure that the attorney-client privilege will be properly identified and assessed, and will help to prevent inadvertent waiver of the privilege.

### **c. Privacy Considerations with the Use of Collaborative Platforms Within the Borders of the United States**

#### **(1) U.S. Privacy Considerations**

Adopters of collaboration platforms must be aware of implicated privacy issues involved in using such platforms which cross state and often global boundaries. While the United States has a mix of federal laws to protect specific types of data, “[it] has no overarching and preemptive national ‘privacy law’ or ‘data security law’ in place.”<sup>36</sup> Generally, at the current time, there is no all-embracing privacy law; privacy in the U.S. is addressed by state-specific laws, and for those states that do have such laws there

---

<sup>36</sup> See Sedona Conference Journal, 22 Sedona Conf. J. 83 at 497 (2021).



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

is a lack of uniformity across such states.<sup>37</sup> *See generally, id.* at 497-505. Communication and collaboration tools are used by multi-state and global entities, so the users may be located in different states and different countries. In the U.S., Courts have found that the law governing the claim asserted in a matter applies with respect to privileges. *See e.g., Lieberman v. Unum Group*, 2021 U.S. Dist. LEXIS 200941, \*5 (C.D. Cal. Oct. 14, 2021) (rejecting arguments that other state's privacy laws apply, deciding that the law underlying the claims and defenses governs). When there are users based in different jurisdictions, consideration should be given to whether and how privacy laws will govern the information and its retention.

Information collected by collaboration platforms may raise additional privacy concerns for personal information - which could be identifying information regarding users, and certainly for information that may be consists of protected health information or other sensitive personal information. While HIPAA protects the disclosure of personal identifiable information, the HIPAA privacy rule only applies to covered entities—namely health plans, health plan clearing houses, and health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards. *See* 45 CFR § 160.102. To the extent a covered entity houses personal identifiable information within a communication or collaboration tool and such information is sought in litigation, then HIPAA may apply. *See e.g., Lillard v. Univ. of Louisville*, 2014 U.S. Dist. LEXIS 201024, \*52 (W.D. Ky. Apr. 4, 2014) (denying request for Slack because, *inter alia*, it would be a potential HIPAA violation if it contains patient information). In such a scenario, it would be wise for the parties to agree on a protective order that complies with the requirements of 45 C.F.R. § 164.512.

## (2) Privacy Considerations With the Use of Collaboration Platforms Outside the United States – General Data Protection Regulation

The use of collaboration platforms may also raise specific foreign data privacy laws and tangentially other foreign laws, such as labor laws, which restrict retention of information about employees. Consideration should thus be given to the identification of the location of information and users of the platforms. Europe has a comprehensive data privacy law, the General Data Protection Regulation (“GDPR”) (Regulation (EU) 2016 of the European Parliament and of the Council of 27 April 2016)), which governs the rights of personal information of its citizens and addresses how data is processed and controlled within the European Union. The GDPR applies to protect its citizens and certain information, such as personal identifying information or sensitive personal information, from any documents, data, or information collected or processed from them while they are in the European Union- whether as an employee or not. Notably, the GDPR can apply to businesses based in the United States if the business has an establishment in the European Union or if the business targets individuals in the European Union for offering goods and services or monitoring their activities. *See generally*, Sedona Conference Journal, Vol. 22, at 284-343 (2021). Where an entity has employees

---

<sup>37</sup> As of March 2024, there were 15 U.S. state laws on Privacy. *See for example*, the California Privacy Rights Act (“CPRA”) Cal. Civ. Code Section 1798.100 et seq., the Illinois Personal Information Privacy Act, (“PIPA”), 815 ILCS 530, the Connecticut Data Privacy Act, (“CTDPA”) Conn. Gen Stat Section 42-522.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

located in the European Union or does business in the European Union, and discovery is sought from a collaboration platform that the entity's employees use, there may be certain information stored within said collaboration tool that is subject to the GDPR provisions on production and furthermore, may limit retention of such information only as necessary to the purpose for which it was created. Understanding the specific collaboration tool, whether user-specific information is collected, how data is shared, where it is maintained and whether user-specific information is collected is necessary to determining whether foreign data privacy laws will apply. It is further worth noting that many Labor Councils in the EU limit the retention period of an enterprise in keeping such communications that contain personal information; compliance is often insisted upon by the governing Council to prevent violation of the Labor Codes and that may be a basis to explain in discovery why certain information is missing for certain contributors to collaborative platforms.<sup>38</sup>

### C. Information Governance Considerations

Collaboration tools have created great efficiency, accessibility, and opportunities for sophisticated workflow management and information exchange within an organization. Collaboration platforms have also enabled greater social engagement and information sharing by employees and an increase in collaborative work productivity. Use of collaboration platforms, however, should involve careful

---

<sup>38</sup>For third party discovery from a communications provider, the Stored Communications Act (18 U.S.C. §§2701, *et seq.*) prohibits disclosure of the contents of communications from electronic communications services or electronic storage—but the prohibition applies only to those who provide an Electronic Communication Service or a Remote Computing Service. 18 U.S.C. §2702(a). Arguably, this may apply to the content of communications on collaboration tools (including chat messages), but only if the request is to a person engaged in such services.

Because the Stored Communications Act only applies to those providing specified services, it will not apply where the party does not provide such services and the information is within the party's control. *See e.g., Flagg v. City of Detroit*, 252 F.R.D. 346, 354-55 (E.D. Mich. 2008) (in considering a motion to quash a subpoena to a third-party electronic communication service with whom the Defendant had a contract for text messaging, the court determined that the Defendant had control over the text messages such that they should be produced in accordance with Rule 34). But it may apply to a third-party subpoena seeking information that is outside the control of the party and/or outside the scope of the party's business. *See Shemwick v. Twitter, Inc.*, 2018 U.S. Dist. LEXIS 22676, \*6 (N.D. Cal. 2018) (denying plaintiff's request to search the Twitter direct messages of Twitter's custodians because "Twitter did not require its employees to use direct messages for communication").

Title I of the Electronic Communications Privacy Act (18 U.S.C §§ 2510, *et seq.*) prohibits the intentional actual or attempted interception, use, disclosure, or "procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication." 18 U.S.C § 2511. There are exceptions, however, for operators and service providers for uses "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service" and for "persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978." 18 U.S.C. § 2511.



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

consideration to the implementation of appropriate data and information governance principles that apply to that use.<sup>39</sup>

An organization should understand collaboration tools prior to their deployment and use, including whether and how such tools fit within the organization's business processes and information systems (e.g., requirements for records retention, audit, and discovery in litigation). This is commonly accomplished, for example, through the creation of a team that works together to vet the collaboration platform and to understand its capabilities and the provider offering the tool.<sup>40</sup> An organization should have a representative from the legal department either on the team or to provide input to the team to ensure consideration of potential issues that may arise from the collaboration platform's functionalities, including the eDiscovery capabilities and limitations at different license levels. Information or data governance programs should align with the objectives of the organization while maintaining enough flexibility to respond to changes and opportunities.<sup>41</sup>

If an organization is considering a collaboration platform, the team vetting the platform should understand the needs of the users and business units and understand the business, legal and regulatory requirements of the platform. The vetting team should consider whether the collaboration platform has certain functionality, including information retention, preservation, and legal hold, to ensure that the organization understands the platform's capabilities and its use within the organization.<sup>42</sup> Consideration should also be given to the potential need for third-party services that can provide technological capabilities needed to satisfy data preservation, extraction, and review from the platform.<sup>43</sup> The administrator or designated "owner" of the platform within an organization,<sup>44</sup> as well as the legal eDiscovery team and any other relevant business unit authorized to access the administration of the platform should understand where the collaboration platform's data is stored,

---

<sup>39</sup> The Association of Records Managers and Administrators ("ARMA International") sets forth as their highest level of Records Management Principles- Level 5- Transformational- as follows: This level describes an organization that has integrated records management and its infrastructure and business processes such that compliance with the organizations' policies and legal/regulatory responsibilities is routine.

<sup>40</sup> See Principle 1 of the 2019 Sedona Conference Commentary on Information Governance, Second Edition) 20 SEDONA CONF. J. 95 (2019); McKinsey Digital Designing Data Governance that Delivers Value, Ex. 2, by Bryan Petzold, Matthias Ruggendorf, Kayvaun Rowshankish and Christopher Sporleder.

<sup>41</sup> 2019 Sedona Conference Commentary on Information Governance, 20 SEDONA CONF. J. 95 (2019) at 116.

<sup>42</sup> While Courts have not included in their decisions reference to Information Governance as it pertains to collaborative or communication platforms used, they have explicitly ordered E-Discovery from any emerging communication platform used within an organization, e.g. *Mobile Equity Corp. v. Walmart, Inc.* 2:21-cv-00126-JRG-RSP (E.D. Tex. Jan. 4, 2022).. It was implicit in the Court's ruling that now ESI sources are relevant in litigation, and the content and information must be able to be produced...in litigation. Accordingly, customized E-Discovery workflows must exist or be created for the emerging communication platforms that will be a source of ESI. See also *Red Wolf Energy Trading, LLC v. Bia Capital Management, LLC*, Civil Action No. 19-10119-MLW, 2022 WL 4112081, at \*1 (D. Mass. Sept. 8, 2022) where the Court found vendor's and eDiscovery processing tools available as well as SLACK's built-in search functionality to refute Defendant's claim that there was "no ready mechanism to search and produce SLACK messages."

<sup>43</sup> See *Red Wolf Energy Trading* 2022 WL 4112081, at \*1.

<sup>44</sup> Defined as the employee who is given responsibility for the operating, overseeing and maintenance of the tool.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

who has access to it, how it is accessed, and how the data may be preserved, collected, reviewed, and ultimately produced.<sup>45</sup>

A collaboration platform's records retention policy should be clear regarding information and content that may be created on the platform, and the policy should align with the organization's record retention policies. As with all retention policies, they should establish a records retention period for created content as well as different types of messaging components (i.e., email, chat). The records management owner should also take into consideration legal, business, privacy, and regulatory requirements for the retention of content or communications.

An organization should determine if the collaboration platform has the capability to preserve information subject to legal hold, and the manner in which the tool can implement such preservation.<sup>46</sup> The stakeholders should create a strategy to create and release legal holds on information and work product in the platform.<sup>47</sup> The collaboration platform should have the ability of auto-deletion or to purge data when the retention period is expired and when a legal hold is lifted.<sup>48</sup> To ensure the ability to comply with eDiscovery obligations, data about usage and ability to access data, file sizes, searching capabilities across the collaboration platform or its components, as well as exportability are data points that should be available and readily communicable as a prerequisite for implementing such platforms.

An organization should create best practices for collecting and extracting content from collaborative platforms as these tasks are an important part of a company's well-crafted information governance plan and will be necessary when discovery arises. It is important that an organization understands which collaboration tools are being used, which parts of the organization are using these tools, what information is being created in them, and in what form and locations it is being maintained.

Once a collaborative platform is selected and a directive is given across the organization to use the platform as a method of work collaboration, there should be clearly communicated acceptable use standards, including retention standards, and education across the organization on the version of the platform being used, its capabilities, and the approved scope of its use.<sup>49</sup>

Finally, creating a long-term retention strategy appropriate to the value and type of information created or used on the collaboration platform involves considering a broad range of factors pertaining to the digital assets and the circumstances of the organization itself. These factors should include business value, regulatory importance, legal requirements, global and local privacy concerns, intended retention schedule, legal hold status, file format, continued availability of the technologies required to access and read, the likely failure rate of the storage medium as it is configured, the available budget and

---

<sup>45</sup> ABA June 20, 2023, Not Your Same Old E-Discovery Reminder- Be Ready for Discovery of Collaborative Tech and Social Media, by C. Jade Davis.

<sup>46</sup> The Sedona Conference Commentary on Legal Holds, "The Trigger & The Process" Vol. 20, 2019. Second Edition.

<sup>47</sup> Id.

<sup>48</sup> Id.

<sup>49</sup> What is.com Acceptable Use Policy (AUP) by Paul Kirvan.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to [comments@sedonaconference.org](mailto:comments@sedonaconference.org)

resources of the organization, for the tool and/or (for third-party services such as cloud storage, software as a service, etc.), the contractual agreements between the customer and provider.

DRAFT