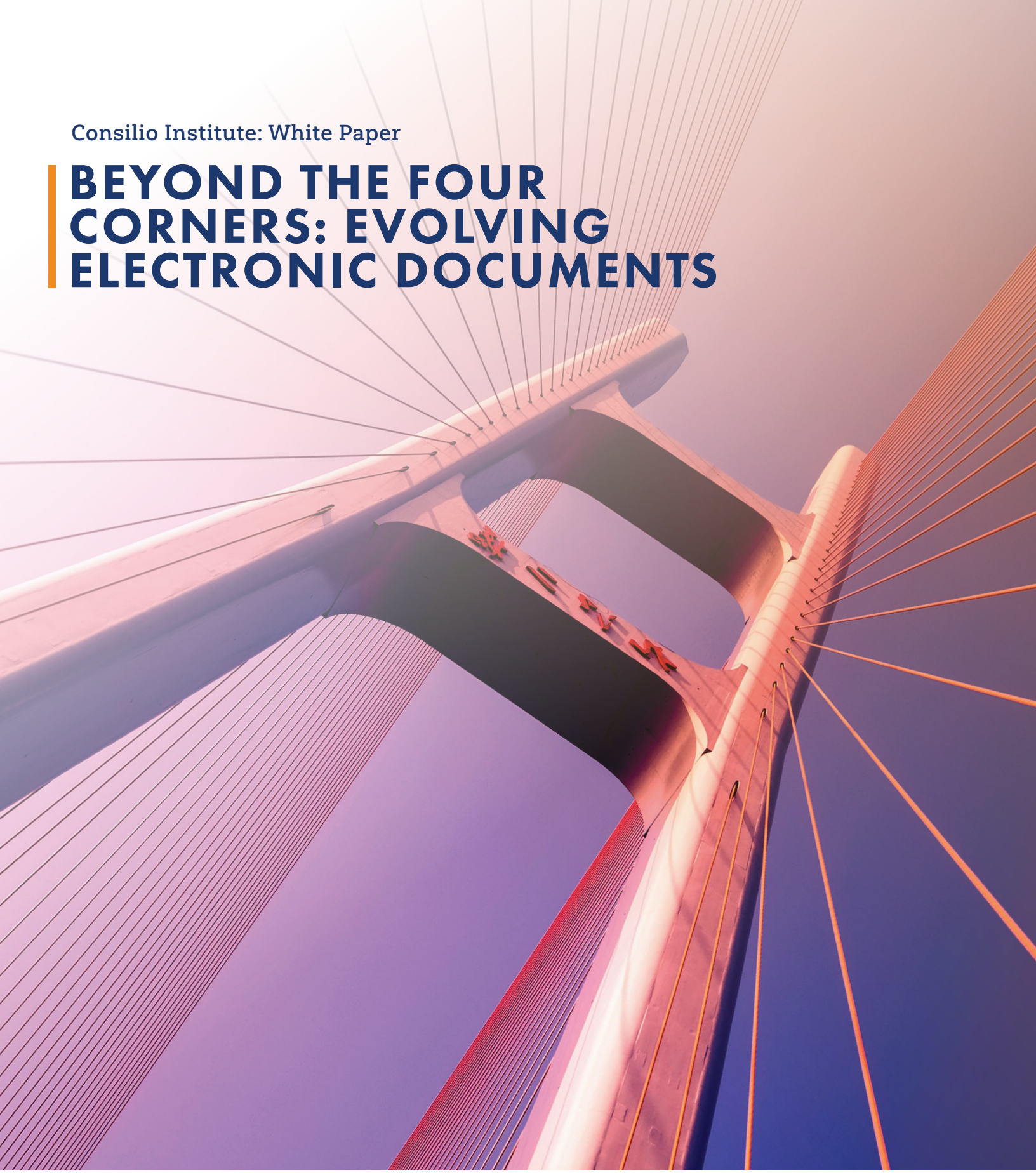
Consilio Institute: White Paper

BEYOND THE FOUR CORNERS: EVOLVING ELECTRONIC DOCUMENTS



Matthew Verga
Director of Education

Mark Garnett
Senior Vice President, DFES

with additional contributions from
Sophie Beattie, Jennifer Knox, and Mike Gutierrez

Consilio / ADVANCED LEARNING INSTITUTE

Consilio / ADVANCED LEARNING INSTITUTE

Consilio Institute: White Paper

BEYOND THE FOUR CORNERS: EVOLVING ELECTRONIC DOCUMENTS

CONTENTS

THE ONLY CONSTANT IS CHANGE

Identification and preservation are the first and most fundamental phases of an electronic discovery effort. Almost every other type of discovery process failure can be fixed with adequate time and money, but once unique, relevant electronically-stored information (ESI) is gone, it's gone. Unfortunately, the challenges of identifying, preserving, and collecting relevant ESI continue to grow as old sources evolve, new sources emerge, and the behaviors of organizations and individuals adapt.

Evolution of Sources and Behavior

The story of the past decade has been one of the long, slow march into the cloud, as organizations have transitioned to new software-as-a-service solutions and individuals have transitioned to new messaging and collaboration tools. One of the clearest illustrations of this trend is the adoption and evolution of the Microsoft 365 offering and the Microsoft Teams application.

Microsoft 365

In 2011, Microsoft launched a new, cloud-based subscription service called Office 365 consisting of their Microsoft Office productivity applications. Office 365 allowed employees and organizations to utilize up-to-date online versions of Microsoft Office applications like Outlook, Excel, Word, and PowerPoint to create their business communications and documents.

Adoption was rapid, and personal, educational, and small business licensing packages followed. By October 2019, Microsoft surpassed 200 million commercial monthly active users.[1] As adoption increased, the range of included applications and capabilities expanded, and by early 2020, Microsoft transitioned to the broader name Microsoft 365 (M365).

A major turning point came in 2020, when the pandemic and the accompanying transition to remote or hybrid work accelerated adoption and usage even more. As of April 2022, Microsoft reported 345 million paid seats for Microsoft 365 and a 17% year-over-year increase in revenue from Microsoft 365.[2] It was also reported that it was in use by over a million companies worldwide,[3] over 870,000 of which were in the United States. As of September 2022, Microsoft

[1]Mary Jo Foley, "A new Microsoft cloud category to watch: The Microsoft 365 number," ZDNET (Oct. 23, 2019), available at https://www.zdnet.com/home-and-office/work-life/that-big-microsoft-365-teams-and-outlook-outage-heres-what-went-wrong/.
[2]Tony Redmond, "Office 365 Reaches 345 Million Paid Seats," Office 365 for IT Pros (Apr. 28, 2022), available at https://office365itpros.com/2022/04/28/office-365-number-of-users/.
[3]Lionel Sujay Vailshery, "Number of Office 365 company users worldwide 2022, by country," Statista, (Feb. 23, 2022), available at https://www.statista.com/statistics/983321/worldwide-office-365-user-numbers-by-country/.

365 customers were adding "over 100 petabytes of new content each month."[4]

Microsoft Teams

As part of the expansion of what would eventually be called M365, Microsoft added in 2017 a new chat and collaboration application called Teams. Teams was created to compete with Slack, which was a self-described "digital HQ" merging communications, information, and documents into a single collaboration application. After its launch in 2013, Slack was the fastest-growing workplace software ever, topping 500,000 daily users in 2015.[5] Despite Slack's four-year head start, however, Microsoft Teams quickly surpassed Slack, reaching 20 million daily users by November 2019.[6]

This rapid growth was then turbocharged by the pandemic and consequent shift to remote and hybrid work, resulting in geometric growth for Microsoft Teams. Daily active users tripled in 2020, and then they more than doubled again in 2021. By the end of 2022, Teams had over 270 million monthly active users.[7]

ABOUT THIS WHITE PAPER

This paper will review key issues for practitioners to consider regarding the challenges created by new and evolving ESI sources. We will begin with current challenges created by the evolving nature of electronic "documents" that cut across source types, and then we will discuss some source-specific issues of which practitioners should be aware.

EVOLVING ELECTRONIC DOCUMENTS

The rapid changes described above have created four major types of preservation and collection challenges that cut across a variety of newer source types: linked and dynamic ESI, threaded message ESI, emojis in ESI, and ephemeral and encrypted ESI.

Linked and Dynamic ESI

As a result of the ongoing transition to more dynamic, cloud-based office and collaboration tools, the old conception of "documents" and "document families" as static things is giving way to a new paradigm in which documents are dynamic and family relationships are virtual.

Traditionally, a document was attached to an email or other message as a self-contained unit containing the data of both the parent email and the child attachment. The relationship between these two electronic documents was easy to preserve and collect. Now, so-called "modern attachments" have changed how this works.[8]

Modern attachments (or pointers, or links) are a feature of Microsoft OneDrive for Business that integrates with Microsoft Outlook clients and Teams clients, and versions of the same functionality are being implemented in other platforms such as Google Workspace and Adobe Cloud. Instead of attaching a copy of a document to an email message, the system inserts a link to the original document that a recipient can click to open it directly.

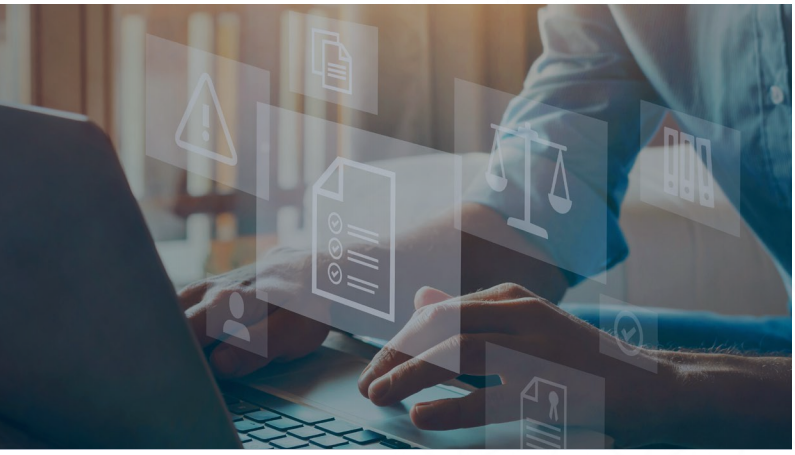
[4]Omar Shahine, "Microsoft is recognized as a Leader in the 2021 Forrester Wave for Content Platforms," Microsoft 365 Blog (Sept. 28, 2021), available at https://www.microsoft.com/en-us/microsoft-365/blog/2021/09/28/microsoft-is-recognized-as-a-leader-in-the-2021-forrester-wave-for-content-platforms/.
[5]Jack Linshi, "This 1-Year-Old Startup Says It's the Fastest-Growing Business App Ever," Time (Feb. 12, 2015), available at https://time.com/3705218/slack-business-app/.
[6]Mary Jo Foley, "Microsoft says it has 20 million daily active Teams users," ZDNET (Nov. 19, 2019), available at https://www.zdnet.com/article/microsoft-says-it-has-20-million-daily-active-teams-users/.
[7]Lionel Sujay Vailshery, "Microsoft Teams: number of daily active users 2019-2022," Statista (Jan 13, 2023), available at https://www.statista.com/statistics/1033742/worldwide-microsoft-teams-daily-and-monthly-users/.
[8]Staci Kaliner, Monica McCarroll, and Ben Barnes, "Let's Start by Calling Them What They Are for Discovery: 'Pointers' Not 'Modern Attachments,'" Legaltech News (Aug. 11, 2022), available at https://www.law.com/legaltechnews/2022/08/11/lets-start-by-calling-them-what-they-are-for-discovery-pointers-not-modern-attachments/.

This new paradigm presents several open questions for electronic discovery:

- Should a linked document be treated the same way as a traditional attachment?
- What if the current version of the document is different than when the link was sent?
- Are parties required to try to recover or recreate past versions of the document?
- What is the right balance between burden and reasonableness in this context?

Courts have not yet reached a consensus on the question, with some ordering the production of linked documents and some declining to do so.[9] What the analyses so far have in common is a fact-specific focus that looks a lot like a traditional proportionality analysis. Factors considered have included the language of the discovery agreement between the parties, the scope of the specific request, the technical or financial burden of fulfilling the request, and the importance of the linked documents.

Beyond linked attachments, other types of dynamic content are also creating new challenges. For example, what is the right way to preserve, collect, and produce particular views of a dynamic dashboard?[10]



Threaded Message ESI

Traditionally, organizations treated enterprise email as foundational to their information management and eDiscovery programs and treated chat and messaging applications as casual and secondary. Today, a major transition is under way from email communication to chat and collaboration tool communication, and the younger an employee is, the more likely they are to prioritize these new communication channels over traditional email.

The proliferation of mobile device sources, social media sources, and collaboration tool sources has made message thread unitization a common question for eDiscovery. These source types frequently include ongoing threads of back-and-forth messages (e.g., WhatsApp text message threads, social media direct message threads, Slack channel threads, etc.), which can span extended periods of time. Although the specifics vary by source, these message threads are often maintained in ongoing logs that are not conducive to efficient review or later use as evidence. Rather than present weeks or months of messages in a single document, it is typical to unitize these logs into separate, shorter documents for review and production.

When doing so, some judgment must be exercised about what size the units should be. Individual messages stripped of thread context are also not ideal (as courts have pointed out[11]), so some middle ground between massive logs and single messages is preferred. It is common to unitize such materials into 24-hour chunks, so that each day's communications become a single document, but other divisions may be rational depending on your materials and case.

This unitization is typically performed during processing, prior to ECA, review, and production, but production implications should be considered when

[9] See e.g., *Nichols v. Noom, Inc.*, 2021 WL 948646 (S.D.N.Y. Mar. 11, 2021), available at https://app.ediscoveryassistant.com/case_law/32615-nichols-v-noom-inc; *IQVIA Inc. v. Veeva Systems, Inc.*, 2019 WL 3069203 (D.N.J. Jul. 11, 2019), available at https://app.ediscoveryassistant.com/case_law/24806-iqvia-inc-v-veeva-sys-inc.

[10] *Famulare v. Gannett Co.*, 2022 WL 815818 (D.N.J. Mar. 17, 2022), available at https://casetext.com/case/famulare-v-gannett-co.

[11] See, e.g., *Laub v. Horbaczewski*, 331 F.R.D. 516 (C.D. Cal. Apr. 22, 2019) (Magistrate Judge expressing a preference for "aggregated" formats preserving "the integrity of the threads of communication reflected in the text messages"), available at https://casetext.com/case/laub-v-horbaczewski.

making the determination, as parties can disagree over the best way to unitize and produce such materials.

Emojis in ESI

Over the past decade, adoption of emoji use has become widespread. By 2019, according to a survey report from Adobe,[12] more than 90% were using emojis in personal communications, and more than 60% were using emojis in work communications. For example, according to a Microsoft spokeswoman,[13] emoji use in 2019 was "basically universal" among the 13 million daily active users of Microsoft Teams.

As these communication channels have become more frequent discovery sources, so too have emojis shown up more frequently in cases. In 2019, Santa Clara University Professor of Law Eric Goldman published "Emojis and the Law"[14] in the Washington Law Review, which revealed that "[b]etween 2004 and 2019, there was an exponential rise in emoji and emoticon references in US court opinions."[15] The presence of these emojis creates special challenges for eDiscovery and litigation – both technical challenges and challenges of interpretation.

First, the volume and diversity of emojis make it a challenge for discovery tool developers and service providers to keep up with supporting them all. There are an enormous and growing number of emojis, and they work in a variety of ways. The cross-platform emojis recognized by the Unicode Consortium exist as alphanumeric codes that various software knows to replace by displaying a corresponding image, while platform-specific and user-created emojis may be based on custom, platform-specific codes, or may exist only as image files that function more like attachments. This support problem even extends to the word processing software used to write briefs and opinions and to the search tools powering case law databases.

Second, there is a challenge associated with the contextual relationship between emojis and text when they are used together. If included emojis are not all captured and displayed, it can lead to material alterations to messages and their meaning. For example, a message might include an emoji indicating it was intended humorously or sarcastically. If that emoji is omitted during collection or not displayed during review, the message might appear misleadingly serious or literal. Communications using multiple emojis can also be very ambiguous. It may not be clear to you what a custodian was attempting to communicate or what a recipient understood.

Ephemeral and Encrypted ESI

Another change over the past decade has been the increase in availability and use of ephemeral messaging and end-to-end encryption. Ephemeral messaging allows for the automatic deletion of sent messages after a set amount of time. As far back as 2016, ephemeral messaging applications were being used by 56% of smartphone owners ages 18-29,[17] and in 2017, Uber made headlines[18] for its use of ephemeral messaging app Wickr, and they were not alone.[19]

Ephemeral messaging can have advantages for organizations, including reducing unnecessary data retention and increasing the security of sensitive communications. When it comes time for discovery or investigation, however, ephemeral messaging can create challenges. First, all automatic deletion of new relevant communications must be suspended, which may be difficult if central control of the relevant channels' settings is not possible. Second,

[12] Adobe, *Emoji Trend Report 2019*, (Jul. 15, 2019), available at https://www.slideshare.net/adobe/adobe-emoji-trend-report-2019.
[13] Christopher Mims, Yes, *You Actually Should Be Using Emojis at Work*, WALL STREET JOURNAL (July 20, 2019), available at https://www.wsj.com/articles/yes-you-actually-should-be-using-emojis-at-work-11563595262.
[14] Eric Goldman, *Emojis and the Law*, 93 WASH. L. REV. 1227 (2018), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3133412.
[15] Dami Lee, *Emoji are showing up in court cases exponentially, and courts aren't prepared*, THE VERGE, https://www.theverge.com/2019/2/18/18225231/emoji-emoticon-court-case-reference (Feb. 18, 2019).
[16] Today, there are more than 3,500 emojis recognized by the Unicode Consortium. Beyond those cross-platform emojis, many platforms also include platform-specific emojis or allow for the creation of custom emojis. In popular collaboration tool Slack, for example, "26 million custom emojis have been created since the feature was introduced."
[17] Greenwood, Perrin, & Duggan, *supra* note 16.
[18] Julie Bort, Uber's *CEO acknowledged his workers' use of secretive messaging apps — and says he banned them*, INSIDER, http://www.businessinsider.com/ubers-new-ceo-has-banned-secretive-messaging-apps-2017-11 (Nov. 29, 2017).
[19] Heather Kelly, *Secret message apps on the rise at work*, CNN BUSINESS, http://money.cnn.com/2017/12/11/technology/secret-messaging-apps-work/index.html (Dec. 11, 2017).

a company's intentions may come under scrutiny – particularly in the absence of clear usage and retention policies – if there is some question as to why certain communications were being deleted.

Properly implemented end-to-end encryption, on the other hand, protects messages by ensuring it's impossible for anyone but the sender and recipient to read them. Availability and use of this has also been on the rise. For example, encrypted messaging app Signal has been one of the fastest-growing new communication platforms in the world. As of the end of 2021, it had more than 40 million monthly active users,[20] and many of them were using it for both private and professional communications.

As adoption and use has increased, so has the frequency with which Signal has been identified as a source of relevant communications that must be identified, preserved, and collected to fulfill litigation duties, compliance duties, and other recordkeeping obligations. Government agencies have recently placed special emphasis on the importance of organizations accounting for all communication channels in use by their employees, particularly encrypted or ephemeral channels like Signal.[21]

End-to-end encrypted applications like Signal pose a variety of challenges as discovery sources. Data is typically available only from the users' devices and only with the users' credentials. In some cases, it is only possible to collect the data by gaining root access to the mobile device or by using expensive specialized tools. Often, the best option is "collecting" via screen captures or screen recordings, which can then be run through optical character recognition and manually annotated with relevant metadata.

SOURCE-SPECIFIC ISSUES

Beyond the four cross-source issues discussed above, it is also important for practitioners to be aware of some source-specific challenges associated with the five sources most commonly associated with the issues above. They are mobile devices, OTT messaging apps, collaboration tools, Microsoft 365, and social media.

Mobile Devices

Mobile devices – smartphones in particular – have become ubiquitous for both personal and business life. Like all consumer technology, there are a plethora of models and types available, and new ones are released by each maker each year. And, because many organizations have adopted bring-your-own-device policies (BYOD), organizations may have a much wider variety of smartphones as potential sources than computers (which still tend to be organization-selected and issued).

Smartphones are more difficult, more costly, and more time-consuming to collect and process than computers. The difficulty, cost, and time can vary from model to model, from maker to maker, and from operating system to operating system. Collection directly from smartphones requires specialized tools like those used to collect from a custodian's computer. Collections instead from cloud-based backups of the smartphone in question are sometimes also an option.

Different models run different types of operating systems, and the operating systems differ in functionality and are updated regularly. Updates can affect the way in which applications store their data or how they are backed up. In other words, data that can be forensically extracted today, may not be able to be extracted tomorrow, or vice versa.

At a high level, applications that come pre-installed on a mobile device when you take it out of the box and

[20] David Curry, "Signal Revenue & Usage Statistics (2023)," Business of Apps (Jan. 9, 2023), available at https://www.businessofapps.com/data/signal-statistics/.
[21] See, e.g., Matthew Goldstein and Emily Flitter, "Texting on Private Apps Costs Wall Street Firms $1.8 Billion in Fines," The New York Times (Sept. 27, 2022), available at https://www.nytimes.com/2022/09/27/business/banks-fined-texting-sec.html; U.S. Department of Justice, "Evaluation of Corporate Compliance Programs (Updated March 2023)" 17-18 (Mar. 3, 2023), available at https://www.justice.gov/criminal-fraud/page/file/937501/download.

power it on, such as Contacts, SMS, MMS, Calendar, Photos, and Video, will typically be extracted from the handset during a standard imaging process using forensic tools. These applications are known as "stock" applications.

Additionally, it is important not to overlook less common mobile devices that may, at times, be relevant, such as vehicle GPS or data systems,[22] wearable devices like fitness trackers,[23] etc.

OTT Messaging Apps

Third-party applications on mobile devices, which are applications that the user downloads onto the handset from digital storefronts like the Apple App Store or the Google Play Store, may or may not be extracted from the handset during a standard device collection process. As noted above, this may be because of end-to-end encryption or other security measures implemented by the app's developers.

This varies not just from app-to-app but even across devices and operating systems. For example, WhatsApp data is stored in an encrypted format on recent Android devices and cannot be extracted as part of a standard mobile phone imaging. This is not the case with iPhone, where WhatsApp data could be captured in a readable format.

Some third-party applications store data within the cloud as opposed to on the user's device. Data from these applications cannot be extracted from a user's device during a standard collection. Applications that store data within the cloud may require separate standalone collections directly from the cloud services.

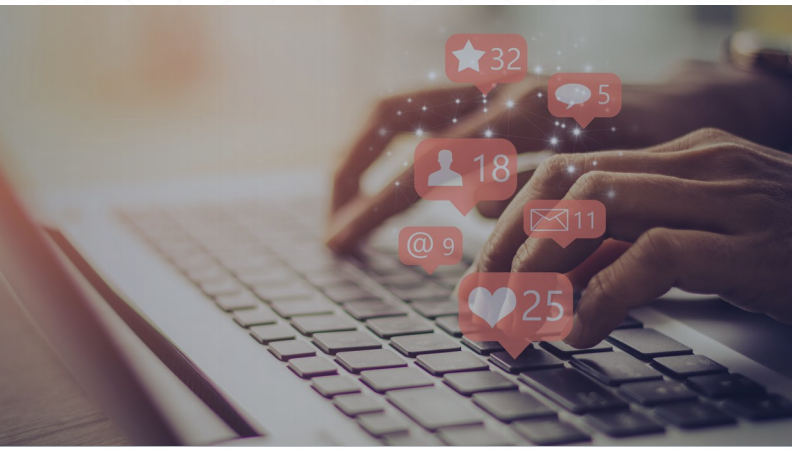
Collaboration Tools

Collection from collaboration tools like Slack and Teams requires navigating a collection of diverse sources, containing diverse content, and potentially, stored in diverse locations. Relevant communications may exist in public channels, private channels, direct messages, or group messages. It is not uncommon for an organization to have channels numbering in the thousands and messages numbering the millions. Moreover, each message may contain reactions, animations, links to videos, embedded content from third-party sources, and more.

Another challenge arises from the variety of licenses available. The type of license under which an organization uses Slack will dictate what options are available for preservation and export of relevant materials. For example, a free license for Slack caps how many messages can be preserved and exported, while paid licenses do not. Paid licenses also allow for more granular preservation options. In Teams as well, the Microsoft 365 license under which an organization uses Teams will determine what preservation and export tools are available.

An additional challenge arises from the diversity of places where relevant data may reside, which can complicate preservation and export. For example, different types of Teams data are stored in different places within the Microsoft 365 environment. Individual Teams content is stored in a user's mailbox, non-private channels content is stored in the group mailbox used for the team, and other types of content

[22] David Horrigan, *e-Discovery Spoliation in Unusual Places: Preserve Your Pickup Truck*, RELATIVITY BLOG, https://www.relativity.com/blog/e-discovery-spoliation-in-unusual-places-preserve-your-pickup-truck/ (Mar. 2, 2017).
[23] Katherine E. Vinez, The Admissibility of Data Collected from Wearable Devices, 4 Stetson J. Advoc. & L. 1 (2017), available at https://www2.stetson.edu/advocacy-journal/wp-content/uploads/2017/06/Vinez_-_Wearables.pdf.



are stored in various SharePoint and OneDrive locations. In Slack or Teams, embedded content may be stored in third-party applications (e.g., Dropbox, YouTube) and just displayed dynamically based on the link that's actually in the message.

Because of these challenges and variations, as well as the additional challenges that arise during processing (e.g., expansion, format conversion, unitization), successful collection from these kinds of sources typically requires the assistance of an experienced collection expert, and it may require custom solutions.

Microsoft 365

Preservation in and export from Microsoft 365 presents the same challenges discussed above for Teams. It encompasses a wide range of sources and date types. It can contain enormous numbers of files and enormous volumes of data. Preservation and export options are dictated by license level, and they are complicated by the diverse array of places different types of user data is stored – both inside the Microsoft 365 environment and in third-party applications. Successful collection from these kinds of sources typically requires the assistance of an experienced collection expert (as well as the cooperation of the account holder, for individual accounts), and it may require custom solutions.

Social Media

For better or worse, social media is an influential, indispensable part of modern life. As it's permeated its way ever deeper into our professional and personal lives, its impact upon discovery has grown in parallel. In April 2019, the International Legal Technology Association published the results of its 2018 Litigation and Practice Support Survey,[24] revealing that 90% of responding professionals (overwhelmingly from law firms) had handled at least one case involving the collection and processing of social media data in the prior year, a 7% increase over the prior year.[25] Moreover, 19% reported handling more than 20 such cases, a 46% increase over the prior year.

Social media sources can pose technical challenges because they typically incorporate multiple forms and formats of media and communication together, creating a complex source of diverse ESI. They commonly allow sharing of photos and videos, status updates, public posts, private messages, live chats, video streams, and more. In addition to the material posted and uploaded by users, social media services also record extensive information[26] about each user's activities on the service, such as what content they've liked or shared, logs of when and how they've accessed the service, and sometimes more.

All of this material accumulates rapidly into large volumes because social media users access these services frequently and share hundreds of millions of new posts, messages, photos, and videos every day. Each individual social media account for each user can easily contain hundreds or thousands of pages of materials in a mishmash of formats. Facebook, for example, published a paper in 2021 on its transition to a new file system for its data centers[27] in which each cluster "scales to exabytes," up from "tens of petabytes" in their previous system.

[24] Cindy MacBean, *2018 Litigation and Practice Support Survey Results*, ILTA (Apr. 2019), available at http://epubs.iltanet.org/i/1108621-lps19/36?_ga=2.231156186.434461956.1629978821-1135214194.1629978821.
[25] ILTA's 2017 *Litigation and Practice Support Technology Survey Results*, ILTA (Apr. 2018), available at http://epubs.iltanet.org/i/973671-lps18/55?_ga=2.39038435.1141759458.1531162513-441756871.1531162513.
[26] *What categories of my Facebook data are available to me?*, FACEBOOK HELP CENTER, https://www.facebook.com/help/405183566203254?helpref=faq_content (2021).
[27] *Consolidating Facebook storage infrastructure with Tectonic file system*, FACEBOOK ENGINEERING, https://engineering.fb.com/2021/06/21/data-infrastructure/tectonic-file-system/ (June 21, 2021).

There are three main options for the acquisition of social media materials for use in litigation:

- *Printing out the material or capturing a screen image of it* – this is fast and inexpensive, but it does not capture any native files or metadata. It may also create authentication and admission problems down the road.
- *Using the self-service export tools provided by the social media platform* – this, too, is fast and inexpensive, but it also may not provide native files or metadata. It often comes in a format that requires conversion using forensic tools, and not all parts of the content may be exported in a way that facilitates that conversion.
- *Using specialized forensic collection software* – this carries additional costs, but it can be essential for cases involving large quantities of social media materials, questions best resolved through the materials' metadata, or the potential for disputes over the authenticity and admissibility of the social media materials themselves. Escalating security and privacy measures, however, have begun to reduce how much these tools can do beyond the standard export function.

CONCLUSION

The challenges of identifying, preserving, and collecting relevant ESI continue to grow as old sources evolve, new sources emerge, and the behaviors of organizations and individuals adapt. The story of the past decade has been one of the long, slow march into the cloud, as organizations have transitioned to new software-as-a-service solutions and individuals have transitioned to new messaging and collaboration tools.

For practitioners, learning about these sources and the challenges they create is no longer optional, as the sources are becoming ubiquitous. The complexity and variability of these ESI sources, however, frequently makes these issues too complex to address without the assistance of relevant discovery or collection experts. Consulting with them early and often is the best way to make sure you know what is technically possible in each situation and how to proceed reliably and defensibly.

ABOUT THE AUTHOR

Matthew Verga is an attorney, consultant, and eDiscovery expert proficient at leveraging his legal experience, his technical knowledge, and his communication skills to make complex eDiscovery topics accessible to diverse audiences. A fifteen-year industry veteran, Matthew has worked across every phase of the EDRM and at every level, from the project trenches to enterprise program design. As Director of Education for Consilio, he leverages this background to produce engaging educational content to empower practitioners at all levels with knowledge they can use to improve their projects, their careers, and their organizations.

Matthew Verga, Esq.
Director of Education
m +1.704.582.2192
e matthew.verga@consilio.com
consilio.com

ABOUT THE AUTHOR

Mark is responsible for managing forensic teams across the US, UK, EU and APAC regions. The forensic team is responsible for the delivery of all forensic collection, forensic data analysis, discovery consulting and expert witness services to both law firm and corporate clients alike. Mark specializes in managing teams responsible for collecting and analysing digital evidence, data recovery, electronic evidence preservation, electronic discovery and expert reporting.

Mark is a qualified investigator, electronic discovery and forensic technology practitioner with 14 years experience as a Detective in the Queensland Police Service and 20 years specialist electronic discovery and forensic experience, six of which were with a “Big Four” forensic practice in Australia. He responsible for the global delivery of forensic services to all of Consilo’s clients.

Mark Garnett
Senior Vice President
m +44 7495455877
e mark.garnett@consilio.com
consilio.com