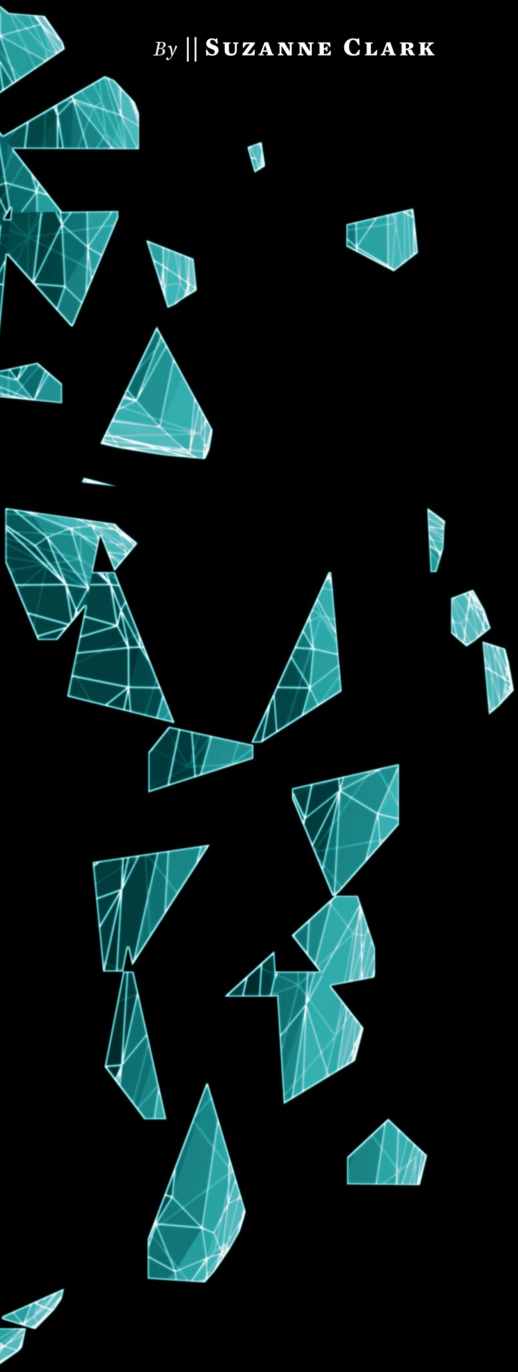
Cracking the Code on ESI

Virtual data is dispersed across more devices, apps, and portals than ever before. Build your case by collecting everything—from messaging apps that auto-delete to cloud-stored documents.

By || **Suzanne Clark**



The volume of "documents" relevant to litigation and government investigations has exploded due to electronic data, leading to a significant shift in the discovery process. What once required a trip to a client's filing cabinets, a banker's box, or an Iron Mountain storage facility has now become an immense task of identifying a wide array of electronic data sources, often called "big data."

These sources include mobile devices, collaboration tools like Microsoft Teams and Slack, text messaging apps, ephemeral (temporary) messaging apps like Snapchat, shared drives, cloud accounts, medical portals, and GPS units, as well as proprietary software applications.

The sheer volume and variety of big data sources present unique challenges in the discovery process. After identifying what electronically stored information (ESI) exists, attorneys must determine how to collect, search, and review it, and, finally, produce and present it for use at depositions and trials.

The Federal Rules of Civil Procedure were amended in 2006 and again in 2015 to account for the presence of ESI as discoverable information in litigation.[1] Proportionality, preservation, and spoliation have become common concepts affecting all types of litigation. "Burden" took on a whole new meaning. "Spoliation" went from being a clear bad actor to someone who simply failed to stop auto-delete after the opposing party implemented a litigation hold.

ESI collections are an essential aspect of the new frontier of e-discovery. Staying on the cutting edge of e-discovery and ESI collections starts with understanding the available tools and technologies. Then, you must determine the right fit for your specific litigation needs by considering the sources, the people involved, the circumstances, and budget, among other factors.

Mobile Device Forensics

As a plaintiff attorney, you are likely concerned about mobile device evidence from both your client and the opposing party. For your client's mobile device evidence, it's crucial to understand what you need to collect and how to collect it competently.

When dealing with a service provider, you will face several options for mobile device data collection, ranging from highly detailed forensic methods to more targeted approaches. The choice depends on what you need from the device and whose device it is.

Mobile devices contain both user-generated content and system-generated data.[2] One or the other—or both—may be relevant to your litigation, and different mobile device collection tools and techniques are available,

PREVIOUS SPREAD AND THIS PAGE: PASHAIGNATOV/GETTY IMAGES

depending on the type of data you need to collect.

Deleted data. If you need data that a user deleted or system-generated data—like a phone's usage data—you will need a full file system (FFS) extraction to collect that ESI. Obtaining an FFS image of a mobile phone entails hiring a qualified forensic examiner who can use specific tools[3] to perform the FFS extraction[4] and has physical access to the mobile device. This means your client must be without their device for several hours or even a day or two. Although an FFS extraction is the most comprehensive and invasive method of mobile device collection, it is not always necessary.

Content. If you only need the content from a smartphone, a logical image[5] may suffice. Service providers can obtain a logical image remotely and in less time than an FFS extraction. Since logical forensics require a lower investment in forensic tools, more service providers will offer it instead of FFS extraction.

However, beware of a service provider that recommends a less forensically advanced collection method. It may want your business but might not have the more expensive tool needed for full forensic collections. It's important to consider the tools your provider has and why it recommends certain methods. The cost of these tools can be significant, so understanding the spectrum—from FFS to logical and targeted collections—is crucial.

Targeted collections. A third option for mobile device collections is targeted collections. Targeted collections selectively gather specific ESI relevant to the litigation instead of collecting all available data from a source.[6] This type of data collection can be done with the mentioned forensic tools using a less invasive collection method. Some software as a service (SaaS) programs and service providers offer targeted mobile device collections through proprietary software.[7]

When it comes to your client's mobile device evidence, understand what you need to collect and how to collect it competently.

Targeted collections may be appropriate when you represent someone in response to a third-party subpoena, where privacy and burden become significant concerns. In such cases, targeted collections balance privacy and costs with the need for relevant data, as third parties are not directly involved in the litigation and the rules require less of them. Or, for instance, in a matter with dozens of custodians where the parties have agreed only to collect their text messages, you may implement targeted collections of only texts from multiple phones.

Self-collection. What about smaller cases, where cost-effectiveness and proportionality are even more important? There are resources that offer guidance on collecting ESI in smaller matters, including mobile collections and some do-it-yourself collection tools.[8] While risks are associated with self-collection, supervising your client's self-collection may be the only viable option in small cases.

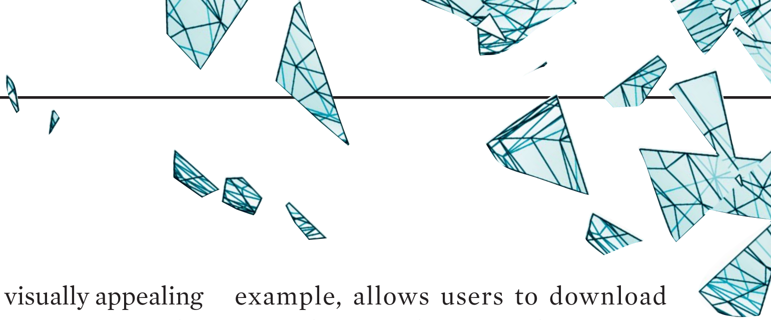
In these situations, ensure you maintain the highest standards for preserving mobile data to allow for a redo if the self-collection is questioned. You should communicate with opposing counsel to agree on self-collection as a cost-saving measure if the amount in controversy is low.

If self-collection is appropriate for your case, you could reach an agreement with opposing counsel that taking screenshots—or using apps that merge screenshots into a single image—is a reasonable solution.[9] Other apps for phone collections, such as iMazing, SMS Backup & Restore, and Dr.Fone,[10] can back up text messages. To minimize costs, have your client record a video while scrolling through text messages. Avoiding overkill in mobile collections is reasonable if you have a solid legal foundation, like a proportionality argument.

Once you take into account and implement the obligations and considerations related to collecting data from your client's mobile devices, you can use that knowledge to hold opposing counsel to the same standard, meet and confer appropriately according to Federal Rule of Civil Procedure 26(f), and recognize when the opposing party's forensic collection efforts fall short.

Social Media Data Collection

Social media platforms such as Discord, Facebook, Instagram, Pinterest, Snapchat, and YouTube are third-party applications[11] that users can access from their devices. The platforms store data in the cloud, though some is also stored locally on mobile devices.



Collecting the device—especially with an FFS extraction—may capture some third-party social media application data. However, to ensure a comprehensive collection of third-party application data from a social media account, you must access the account through the user's login credentials and collect data directly from the account.

Social media users log in and download their data directly from the platform. Privacy laws such as the European Union's General Data Protection Regulation (GDPR)[12] and the California Consumer Privacy Act (CCPA)[13] require companies to give EU and California consumers access to their own data. Platforms offer options like "Download Your Data" (DYD), "Download Your Information" (DYI), or Google Takeout to allow users to collect their data. However, these ESI collections may not include data from other users the account holder interacted with, and the context may be limited. Attorneys and collection providers may use these DYD and Takeout functions to collect ESI from social media platforms for their cases.

A forensic expert can obtain social media collections in various formats, such as JavaScript Object Notation (JSON) or Hypertext Markup Language (HTML), and import them into review platforms. However, reviewing this data can be challenging because it lacks essential context. For example, knowing that someone commented on a post without understanding the content of the post offers limited insight.

Alternatively, some software providers, like PageFreezer and Page Vault, provide comprehensive collection methods for social media platforms.[14] These providers use software to capture the data, offering context and formatting that makes it easier to review.

When collecting your client's social media data, you will use their login credentials, and these tools can collect all available data in a visually appealing format, similar to how it appears on the platform. In contrast, if a third party collects the data, you can access only publicly available information, and private posts and direct messages remain inaccessible.

For opposing parties, defense counsel will supervise the defendants' data collection and review it before producing it in response to your document requests. You may be able to meet and confer with opposing counsel to discuss their collection method for social media data. Knowing the available collection methods will help prepare you for these negotiations.

Risks and benefits of social media data. Social media evidence is easily deleted, so implement preservation measures. Remind your client of their ongoing duty to preserve their social media accounts and post history.[15]

Collecting social media evidence also raises privacy concerns. For example, information about a user's health, political views, or personal relationships may be collected alongside information relevant to the litigation. Mishandling this data could lead to privacy violations or even identity theft. Additionally, you must consider the time and costs of searching and reviewing the collected social media content.

Despite these risks, social media content, when collected defensibly, is a rich source of real-time information. It provides timestamps, geolocation, device information, and other metadata that serve as pivotal evidence in litigation.[16] The content and metadata collected can help create timelines and authenticate evidence.

Cloud-Based Data Collection

For cloud-based data collections, such as from Google Drive, users must log in to the platform. Google Takeout, for example, allows users to download everything in their Google account, including Google Docs, Google Drive, Google Photos, Google Sheets, and YouTube data. This includes videos users have uploaded to YouTube, as well as their subscriptions, comments, and other account activity, which may include links to watched videos.[17] This method provides a comprehensive collection of data stored in a user's Google cloud account.

To collect data from other types of cloud services, such as from Dropbox, a forensic examiner would use specialized forensic tools.[18] Once I identify a trusted and certified forensic examiner, I rely on their expertise to select the appropriate tools and methods for cloud collections and to defend those choices through declaration and testimony.

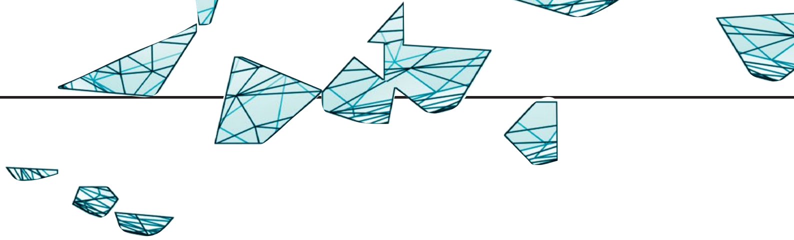
Workspace Collaboration Tools

Corporate defendants commonly use workspace collaboration tools like Slack and Microsoft Teams for productivity and remote access. It's important to know how to collect ESI from these sources and how to handle negotiations regarding the opposing party's use of these tools.

Data collection from these tools presents several challenges.[19] The convenience and productivity they provide often come at the expense of security and e-discovery functions.[20] Additionally, legal technology struggles to keep up with the rapidly evolving features of these platforms. While some of these tools offer built-in e-discovery solutions, service providers can work with these functions to identify issues and ensure defensible collections.[21]

Common e-discovery challenges with these platforms include parties failing to understand the platform or how to search it properly;[22] auto-delete settings; and difficulties associating custodians

PASHAIGNATOV/GETTY IMAGES



with content due to channels, chats, and file sharing. Be aware of these limitations when conferring and assessing incoming productions.

Ephemeral Messaging App Snags

Ephemeral messaging apps like Snapchat or Telegram present significant challenges in preserving relevant ESI. Specifically, can a party with a duty to preserve evidence use these applications to communicate about the litigation without risking accusations of spoliation?[23]

In January 2024, the Federal Trade Commission and the Department of Justice issued guidance on preservation obligations related to these apps. They urged organizations to implement proactive preservation measures to support discovery processes.[24] The key takeaway: Organizations must proactively preserve data by archiving it and training employees on preservation, rather than attempting to collect already deleted ESI.[25]

Forensic examiners can use the same tools and methods that are used for social media data collection to capture and archive any data that remains on ephemeral messaging apps. This includes user DYD collections or tools like PageFreezer and Page Vault.

Technology that creates and stores content is constantly evolving. To maintain technological competence, we can learn about the technology ourselves, hire employees who understand it, or engage service providers or experts.[26] Even when we outsource these tasks, we must have a broad understanding of the technology so we can effectively supervise those who assist us.

We must stay informed about the growing range of ESI sources and the methods for collecting ESI. This requires us to be adaptable and proactive in adopting new tools and strategies to manage ESI collections effectively.

Suzanne Clark *is of counsel at Beasley Allen Law Firm in Montgomery, Ala., and can be reached at suzanne.clark@beasleyallen.com. The views expressed in this article are the author's and do not constitute an endorsement of any product or service by* Trial® *or AAJ®.*

NOTES

[1] *See* Fed R. Civ. P. 1 (2015 amend.); Fed. R. Civ. P. 16 (2015 amend); Fed. R. Civ. P. 16 (2006 amend.); Fed. R. Civ. P. 26 (2015 amend.); Fed. R. Civ. P. 26 (2006 amend.); Fed. R. Civ. P. 33 (2006 amend.); Fed. R. Civ. P. 34 (2015 amend.); Fed. R. Civ. P. 34 (2006 amend.); Fed. R. Civ. P. 37 (2015 amend.); Fed. R. Civ. P. 37 (2006 amend.); Fed. R. Civ. P. 45 (2006 amend.).

[2] Stephen Watts, *Machine Data: An Introduction*, Splunk, Jan. 29, 2024, https://www.splunk.com/en_us/blog/learn/machine-data.html; User-generated data refers to content created by the user, such as photos, videos, text messages, emails, social media posts, and documents. System-generated data refers to content produced by the device's operating system and applications, such as logs, metadata, GPS coordinates, app usage statistics, and system notifications.

[3] For Cellebrite Universal Forensic Extraction Device (UFED), the full forensic suite costs over $30,000. *Cellebrite UFED Series*, SC Media, Oct. 1, 2015, https://www.scworld.com/product-test/cellebrite-ufed-series.

[4] Cellebrite UFED offers multiple data collection methods, including FFS and physical extractions. This tool is widely used by forensic examiners to access and collect comprehensive data from mobile devices, ensuring the integrity and admissibility of the extracted data in legal proceedings. *Cellebrite UFED*, Cellebrite, https://cellebrite.com/en/ufed/.

[5] "Logical forensics involves acquiring data from mobile devices through non-invasive methods. It includes extracting information such as call logs, contacts, messages, and application data. Mobile forensics tools use USB connections or wireless communication protocols to access and collect data from devices without altering the original content." *Best Mobile Forensics Tools*, Forensics Insider, June 3, 2023, https://www.forensicsinsider.com/digital-forensics/best-mobile-forensics-tools/.

[6] Greg Mazares, *The Case for Targeted Smartphone Data Collection*, EDRM, May 3, 2023, https://edrm.net/2023/05/the-case-for-targeted-smartphone-data-collection/.

[7] One such provider is ModeOne. *ModeOne*, ModeOne, https://modeone.io/.

[8] The Sedona Conference, *Primer on Managing Electronic Discovery in Small Cases*, 24 Sedona Conf. J. 93 (May 2023), https://thesedonaconference.org/publication/Primer_on_Managing_Electronic_Discovery_in_Small_Cases.

[9] For example, Tailor and Stitch It! are merge apps. *Id.* at 152.

[10] *Id.* at 152-53.

[11] "Third-party" refers to applications that are not associated with iPhone or Android devices, nor designed by Apple, Google, or other smart phone manufacturers, but are instead created by independent developers. *Third-Party App*, PCMag, https://www.pcmag.com/encyclopedia/term/third-party-app; Maria Webb, *Third-Party App*, Techopedia, Mar. 26, 2024, https://www.techopedia.com/definition/third-party-app.

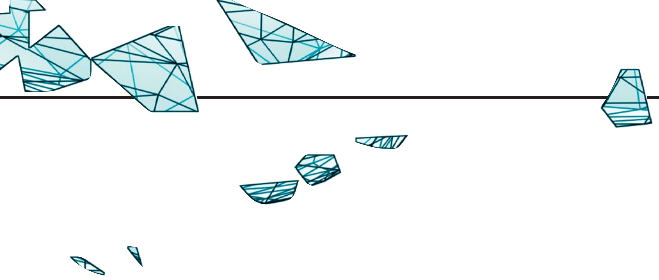
[12] Specifically, under Article 15 of the GDPR, "Data subjects have the right to know certain information about the processing activities of a data controller. This information includes the source of their personal data, the purpose of processing, and the length of time the data will be held, among other items. Most importantly, they have a right to be provided with the personal data of theirs that you're processing." *A Guide to GDPR Data Privacy Requirements*, GDPR.eu, https://gdpr.eu/data-privacy/; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016, Art. 15.

[13] California Consumer Privacy Act (CCPA), Cal. Civ. Code §1798.100; *Frequently Asked Questions*, Cal. Priv. Prot. Agency, https://cppa.ca.gov/faq.html.

[14] These providers use advanced tools to capture and archive social media content, ensuring that all data, including edited and deleted posts, comments, and interactions, are preserved in a forensically sound manner. *Social Media Archiving*, PageFreezer, https://www.pagefreezer.com/social-media-archiving/; *WebPreserver*, PageFreezer, https://www.pagefreezer.com/webpreserver/; *Webpage Capture Software*, Page Vault, https://www.page-vault.com/webpage-capture-software/.

[15] Jennifer Del Medico et al., *Current Trends:*

PASHAIGNATOV/GETTY IMAGES



Discovery of Electronically Stored Information on Mobile Devices and Social Media, Jones Day, June 2019, https://www.jonesday.com/-/media/files/publications/2019/06/current-trends-discovery-of-esi/discovery-of-electronically-stored-information.pdf?la=en&rev=8f2135d18cac48eeb69bf72d65916827&hash=6E2A021742A2258FE62CF0677A5C70CF.

16. *Admissibility of Social Media Evidence: Guidance for Court Cases*, Bosco Legal Services, May 26, 2023, https://www.boscolegal.org/blog/admissibility-of-social-media-evidence-for-court-cases/.

17. *How to Download Your Google Data*, Google Account Help, https://support.google.com/accounts/answer/3024190?hl=en.

18. *Dropbox Forensic Investigations: Logs, Activity Tracking, and External Sharing*, CyberEngage, https://www.cyberengage.org/post/dropbox-forensic-investigations-logs-activity-tracking-and-external-sharing; *eDiscovery Dropbox Collector*, Indexed I/O, Dec. 1, 2015, https://www.indexed.io/blog/ediscovery-dropbox-collector; George O'Brien, *Automating eDiscovery in the Cloud: Dropbox + Guidance Software*, Dropbox Blog, Feb. 5, 2015, https://blog.dropbox.com/topics/product-tips/guidance-and-dropbox-for-business.

19. *Built-In eDiscovery Features for Collaboration Software May Not Be Enough*, Digital Mountain, https://digitalmountain.com/newsletter/built-in-ediscovery-features-for-collaboration-software-may-not-be-enough/.

20. *The Complete Guide to Modern eDiscovery*, JDSupra, July 11, 2023, https://www.jdsupra.com/legalnews/the-complete-guide-to-modern-ediscovery-6207600/.

21. *Built-In eDiscovery Features for Collaboration Software May Not Be Enough*, Digital Mountain, *supra* note 19.

22. *Red Wolf Energy Trading, LLC v. Bia Cap. Mgmt., LLC*, 626 F. Supp. 3d 478 (D. Mass. 2022) (Defendants' delayed Slack productions were due to their failure to engage an e-discovery provider or use appropriate search technologies.)

23. *Case of the Week Episode 31: Don't Ghost When It Comes to Preserving Snapchat Data*, eDiscovery Assistant, July 15, 2021, https://www.minerva26.com/caseoftheweek-episode-31-dont-ghost-when-it-comes-to-preserving-snapchat-data/; *Ephemeral Messaging Data in eDiscovery*, Everlaw, https://www.everlaw.com/guides/novel-data-types/ephemeral-messaging-data-in-ediscovery/.

24. *FTC and DOJ Update Guidance, Reinforces Parties' Preservation Obligations for Collaboration Tools and Ephemeral Messaging*, Fed. Trade Comm'n, Jan. 31, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-doj-update-guidance-reinforces-parties-preservation-obligations-collaboration-tools-ephemeral.

25. Jennifer Joyce & Tracy Tran, *Third-Party and Ephemeral Messaging: Updated Guidelines*, EY, Oct. 1, 2024, https://www.ey.com/en_us/insights/forensic-integrity-services/third-party-and-ephemeral-messaging-updated-guidelines.

26. R. Regulating Fla. Bar 4-1.1.

Estrella de Luz, Bronze, 6.6' x 4' x 0.9', 2022

PASHAIGNATOV/GETTY IMAGES