imageBROKER/Alamy Stock Photo

Ephemeral Messaging: Best Practices for Complying with Discovery Obligations

The use of ephemeral messaging technology has become increasingly widespread. While the temporary or vanishing nature of ephemeral messaging offers many benefits to companies and individuals, it also poses unique challenges, particularly in the discovery process. To properly identify, preserve, and produce relevant ephemeral data in litigation, counsel should understand the main features of ephemeral messaging tools and best practices for managing the discovery-related issues associated with ephemeral data.

SAMANTHA V. ETTARI
SENIOR COUNSEL
PERKINS COIE LLP

Samantha has extensive experience in privacy, data security, and data management issues, including legal, practical, and reputational risk counseling, often in the context of mergers, acquisitions, and technology-driven strategic and investment transactions. She advises clients on domestic and international privacy statutes and regulations, as well as cross-border transfers of data. Samantha is also a seasoned litigator and trial lawyer.

JESSICA TSENG HASEN
SENIOR COUNSEL
PERKINS COIE LLP

Jessica's practice sits at the intersection of traditional legal practice and technology. She counsels clients and litigation teams regarding cutting edge e-discovery issues for complex commercial litigation and government and internal investigations, and also works with clients on litigation readiness and information governance projects. Jessica is passionate about leveraging technology to optimize client outcomes in a defensible and efficient manner.

SAMANTHA KEPLER
SENIOR DISCOVERY CONSULTANT
PERKINS COIE LLP

Sam has wide-ranging e-discovery experience, including in patent, product liability, criminal, and white-collar litigation. She advises clients on ways to defensibly improve effectiveness to create organizational efficiencies that enhance data review and production while implementing cost-saving measures. Sam also analyzes new and complex technology solutions to help build out advanced workflows to address the ever-changing structure and treatment of data as it relates to discovery.

Discovery is a critical component of any litigation, and as corporations and individuals increasingly utilize many forms of communication, courts have quickly embraced new sources of data that are subject to the discovery process. If the data is relevant and accessible, and meets the standards set out in Federal Rule of Civil Procedure (FRCP) 26 (or a state equivalent), the data is fair game in litigation.

As technology advances, and new sources of responsive information continue to emerge, none have yet been as challenging to the discovery process as ephemeral data. Ephemeral messaging tools allow users to automate message deletion in-app (within an application). Unlike traditional messaging software, which allows a user to delete content within their own account but not on the recipient's device, ephemeral messaging gives the user the ability to control the history of content in the application for both the sender and the recipient. As a result, those communication forms are not preserved by design.

Developments in ephemeral messaging can largely be traced to consumer demand for privacy and the desire to replicate the casual nature and impermanence of oral communications. Companies may prefer to use vanishing chat features internally to encourage collaboration and easy communication without the added storage and retention costs. Ephemeral communications exchanged between parties or systems are designed to be nearly instantaneously and automatically deleted, leaving no trace. In some increasingly popular apps (such as Snapchat, Telegram, Hash, Cover Me, Confide, Signal, Wickr, and Wire), messages are ephemeral by default.

Although ephemeral messaging serves many important business and practical purposes, the temporary nature of the data also presents difficulties for preserving, collecting, and producing the data in litigation. This article explains:

- The main features of ephemeral and quasi-ephemeral messaging.
- The business benefits of ephemeral messaging.
- The steps a company should take to properly preserve and collect ephemeral data during discovery.
- The key considerations for producing ephemeral data during discovery.
- The ramifications of failing to preserve and collect relevant ephemeral data in violation of discovery obligations.

FEATURES OF EPHEMERAL AND QUASI-EPHEMERAL MESSAGING

To better understand the challenges and best practices associated with managing ephemeral data in discovery, counsel should be familiar with the main features of ephemeral and quasi-ephemeral messaging.

Search Ephemeral Messaging: Balancing the Benefits and Risks for more on the features of, and variations among, ephemeral messaging applications.

EPHEMERAL MESSAGING

Discovery and privacy think-tank The Sedona Conference has identified certain defining features of ephemeral messaging, including but not limited to:

- Deliberate, permanent, and automated message deletion.
- A robust and unchangeable (or increasingly difficult to alter) deletion trigger.
- No archiving or storage of messages or files.
- An in-app deletion capability that applies to both senders and recipients (which is customizable depending on the application).
- Encryption that restricts third-party access.
- Impediments to retention, such as screenshot warnings or shields to stop collection.

(See The Sedona Conference Journal, The Sedona Conference Commentary on Ephemeral Messaging, Public Comment Version, 22 Sedona Conf. J. 435, 449-50 (Jan. 2021), available at *thesedonaconference.org*.)

QUASI-EPHEMERAL MESSAGING

Quasi-ephemeral messaging refers to communications for which some defining features of ephemeral messaging can be altered. A key feature of quasi-ephemeral messaging is that preservation is possible through:

- Altering deletion and storage settings.
- Retaining metadata.
- The ability to screenshot or capture the communication in another form.

(See The Sedona Conference Commentary on Ephemeral Messaging, 22 Sedona Conf. J. at 451.) The most common ephemeral messaging systems are quasi-ephemeral in that administrators can adjust retention settings and frequently do so at the enterprise level. Examples of quasi-ephemeral messaging applications include Microsoft Teams, Cisco WebEx, and Slack.

In some messaging applications, particularly those integrated with social media platforms (for example, Facebook Messenger, Instagram, WhatsApp, and WeChat), individual users can opt in to ephemerality by choosing a setting that makes their messages automatically disappear after a set period of time or after the message is read.

ADDITIONAL CONSIDERATIONS

Both ephemeral and quasi-ephemeral data present challenges when making search, comprehension, and relevance determinations in discovery. For example, individuals communicating through chat messages tend to:

- Use slang, acronyms, and emojis.
- Move from topic to topic in non-linear fashion without the benefit of introductions, subject headings, or "re:" lines.
- Pick up where oral communications left off or move from one chat medium to another, with little context or framework.

Piecing these conversations together, and identifying their overall subject matter and relevance, can be difficult. Given these challenges, the ability to apply conceptual analytics to

this data form is critical. Many discovery processing and review platforms now can search for emojis, for example, and analytic and concept tools are constantly improving to assist reviewers in identifying thematic or topical threads. However, ephemeral messages cannot and should not be searched, reviewed, and produced in the same manner as email or other static electronic files. Instead, counsel should create a separate workflow for this type of data by first building a complete list of all potential nonstandard data sources (for example, mobile and ephemeral data, among others) that may contain relevant content. Once these sources are identified, counsel should:

- Consider working with a forensic consultant to collect data accurately and comprehensively. The consultant can work directly with custodians or with software support to capture relevant data in a way that is both defensible and can be processed in a reviewable format. However, counsel should weigh whether the efficiencies gained by using any processing tools and review platform applications that group chat data into conversation threads for review and production offset the costs involved.
- Evaluate search terms and determine what adjustments, if any, need to be made for application to chat data, ephemeral or otherwise. In particular, search terms traditionally used to identify potentially attorney-client privileged communications or those protected by the work product doctrine may not be effective for this type of data.
- Consider whether the review criteria to determine whether data is responsive to discovery requests need to be revised to account for the more informal style of communication in messaging applications and use of emojis, images, gifs, and other non-text communication forms.

BENEFITS OF EPHEMERAL MESSAGING FOR BUSINESSES

There are strong business rationales for companies to consider communication channels like ephemeral messaging, including:

- Complying with data minimization requirements found in many privacy statutes and regulations.
- Minimizing data breach exposure.
- Facilitating privacy by design.
- Increasing efficiency and cost savings.

Search Ephemeral Messaging: Balancing the Benefits and Risks for more on the benefits of ephemeral messaging, including enhancing confidentiality, facilitating data minimization, strengthening retention policies, and increasing efficiencies.

LEGAL COMPLIANCE

For decades, many companies were focused on data retention because industry-specific regulations and statutes required retention of information for set and lengthy periods of time. Now, companies are grappling with contradictory legal regimes that encourage or require regular and routine purging of data. For example, the European Union's General Data Protection Regulation (GDPR) and the California Privacy Rights Act (CPRA) require companies to practice data minimization and storage limitation by securely and permanently discarding data that no longer has a legitimate business purpose or is no longer subject to a retention obligation (for more on the GDPR, search Cross-Border Discovery Under the GDPR on Practical Law).

However, law enforcement and regulators have had misgivings about the use of ephemeral messaging because it conflicts with compliance obligations under the Foreign Corrupt Practices Act (FCPA) Corporate Enforcement Policy and the obligations of registered broker-dealers and investment advisers. Agencies that have prohibited, limited, or cautioned against the use of ephemeral messaging include:

- **The Department of Justice (DOJ).** The DOJ initially prohibited organizations being investigated in FCPA matters from using ephemeral messaging in 2017 but loosened the prohibition in 2019, allowing ephemeral messaging use where there is "appropriate guidance and controls" and where it does not undermine "the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations" (DOJ Justice Manual, FCPA Corporate Enforcement Policy § 9-47.120(3)(c), available at *justice.gov*).
- **The Securities and Exchange Commission (SEC).** The SEC continues to recommend that investment advisers prohibit "business use of apps and other technologies that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back up" (SEC Office of Compliance Inspections and Examinations, National Exam Program Risk Alert, Observations from Investment Adviser Examinations Relating to Electronic Messaging, at 3, available at *sec.gov*).

DATA BREACH EXPOSURE

For companies that suffer a data breach or other security incident, the more data the company has, the broader the potential exposure. Some states have therefore incorporated into their data breach statutes proactive storage limitation requirements, including:

- **New York.** In 2016, New York enacted the New York Department of Financial Services (NYDFS) Cybersecurity Requirements for Financial Services Companies, which requires certain financial institutions to develop and implement cybersecurity policies, including "policies and procedures for the secure disposal on a periodic basis of [certain] Nonpublic Information" (23 NYCRR § 500.13; for more information, search The NYDFS Cybersecurity Regulations on Practical Law).
- **California.** The California Consumer Privacy Act of 2018 provides individuals with rights to access and delete their personal information and a private right of action in the event of an actual data breach (for more information, search Understanding the California Consumer Privacy Act (CCPA) on Practical Law).

Consistent with these proactive storage limitation requirements, ephemeral messaging tools minimize the amount of data available to intruders and vulnerable to breach by enabling entities to reduce the amount of data they store.

PRIVACY BY DESIGN

In part because many domestic and international privacy regulations now include data minimization requirements, business and consumer demand for privacy and data minimization is a driving component in new software design, online interfaces and applications, and other consumer or business-to-business tools. As a result, companies creating ephemeral messaging platforms are focusing on how ephemeral messaging tools and communications can facilitate privacy and data minimization at the outset of product design. Instagram's recent "vanishing" mode is just one example of a consumer use.

EFFICIENCY AND COST SAVINGS

Storing large files and voluminous data can be costly and slows systems down. The use of ephemeral messaging can both increase operational efficiency and help avoid the need for costly server expansion or cloud storage by reducing the amount of data preserved and storage space needed.

PRESERVING AND COLLECTING EPHEMERAL DATA

Ephemeral data may be relevant to an investigation, litigation, or other dispute. Therefore, once litigation is anticipated or another triggering event occurs, such as receipt of a third-party subpoena or a regulatory investigation, a company's obligation to preserve that data arises.

To comply with the duty to preserve and enable collection of ephemeral data for use in litigation or an investigation, companies should take certain steps both before and after the duty arises.

Search Duty to Preserve Evidence (Federal) for more on the duty to preserve potentially relevant evidence, including when the duty begins and ends, the scope of the duty, and how counsel and clients can comply with the duty.

Search Reasonable Anticipation of Litigation Under FRCP 37(e): Triggers and Limits for more on the factors for identifying when a party should reasonably anticipate litigation, triggering the duty to preserve.

BEFORE THE DUTY TO PRESERVE ARISES

It may be much easier to comply with the duty to preserve if a company has already taken measures to address proper data retention and destruction before an existing or anticipated lawsuit or investigation, such as:

- Written retention policies that address ephemeral data.
- Acceptable use policies that address the appropriate use of ephemeral messaging tools, including situations in which these communication tools should be avoided due to regulatory compliance or other business rationales.
- Policies addressing individual versus enterprise use of ephemeral messaging tools.
- Bring Your Own Device ("BYOD") policies that address the use of ephemeral messaging tools for personal or corporate use on personal devices.

AFTER THE DUTY TO PRESERVE ARISES

Even if preventive measures or enterprise-level guidance have not been put in place, counsel for a company that is or anticipates being involved in litigation should consider taking the following steps:

- **Suspend use of communication channels that cannot be preserved.** A company that begins or continues to use ephemeral messaging tools after the duty to preserve arises without enabling settings that allow for preservation may face a finding of spoliation and the imposition of sanctions (see, for example, *WeRide Corp. v. Huang*, 2020 WL 1967209, at *9-10 (N.D. Cal. Apr. 24, 2020) (imposing sanctions where the ephemeral messaging tool DingTalk was implemented for intra-company communications following the issuance of a preliminary injunction mid-litigation); *Herzig v. Ark. Found. for Med. Care, Inc.*, 2019 WL 2870106, at *4-5 (W.D. Ark. July 3, 2019) (holding that the defendants' switch to the ephemeral messaging tool Signal mid-litigation and configuration of the tool to delete text messages was "intentional and done in bad faith")).
- **Deploy tools for collecting vanishing data that may still be accessible or backed up.** This is likely only necessary if the data is reasonably accessible at the time litigation is pending or anticipated. If so, the failure to collect the data before it disappeared is difficult to justify and could result in sanctions. (See, for example, *DR Distribs., LLC v. 21 Century Smoking, Inc.*, 513 F. Supp. 3d 839, 979, 982 (N.D. Ill. 2021) (ordering a jury instruction on lost evidence where the defendants failed to preserve Yahoo! chats that could have been cut and pasted into emails to retain their contents); *Franklin v. Howard Brown Health Ctr.*, 2018 WL 4784668, at *4, *6-7 (N.D. Ill. Oct. 4, 2018) (finding that the parties could present evidence to the jury to determine whether the defendant's destruction of and failure to preserve evidence occurred by "mistake or something more sinister" where the defendant could have preserved instant messages by suspending an auto-delete function), report and recommendation adopted, 2018 WL 5831995 (N.D. Ill. Nov. 7, 2018).)
- **Interview custodians who used ephemeral messaging tools.** Counsel should interview these custodians to ascertain:
  - whether any custodian has taken screenshots or used other tools to capture the conversations (see, for example, *Williams v. UnitedHealth Grp.*, 2020 WL 528604, at *2 (D. Kan. Feb. 3, 2020) (holding that the defendant had produced all relevant documents and that there were no further communications to produce where the platform Cisco Jabber/Instant Messenger did not store communications (notably due to the defendant's setting) but the defendant produced screenshots of all of the relevant conversations)); and
  - the nature of relevant communications with as much specificity as possible, which is particularly important in situations where a counterpart may have been taking screenshots or utilizing tools to collect the messages and then using the images to discredit or cross-examine a witness (see, for example, *Waymo LLC v. Uber Techs., Inc.*, 2018 WL 646701, at *21 (N.D. Cal. Jan. 30, 2018) (stating

that the defendant's use of ephemeral messaging channels was relevant as a possible explanation for why the plaintiff failed to turn up more evidence of the defendant's misappropriation of trade secrets in the case)).

- **Memorialize the nature of the data and whether preservation and collection efforts are available, practicable, and proportionate to the needs of the case.** Counsel should consider whether the cost of processing, searching, and producing the data outweighs the requesting party's need for it. If not, a motion to quash may be defensible and preferable to costly data restoration, review, and production (see, for example, *Milbeck v. Truecar, Inc.*, 2019 WL 4570017, at *3 (C.D. Cal. May 2, 2019) (holding that the time and expense required to process Slack data and make responsiveness determinations for the messages outweighed the requesting party's need for the data, particularly in a litigation where significant productions had already been made)).

PRODUCING EPHEMERAL DATA

If ephemeral data can be captured, the format in which parties produce it typically aligns with other recognizable production formats. For example, parties can produce chat messages in image format just like email and other loose data types.

The production protocol parties develop should define:

- **The types of communication within the scope of review and production.** By not specifying what communications should be included, parties run the risk of excluding potentially key data sources. For example, parties can specify the scope of production to include communications in any of the following forms, among others:
  - email;
  - facsimile;
  - text messages (that is, short message service (SMS) messages);
  - messages sent via instant messaging applications; and
  - voicemail.
- **Metadata fields unique to message data that the parties should include in the production.** When message data, such as a chat, is processed, certain fields are parsed out that are required to piece the chat story together. These may include, but are not limited to:
  - the chat participant list;
  - the chat date;
  - the chat room name; and
  - the chat start and end times (and dates, if applicable).

From the requesting party's standpoint, discovery requests should specify early on in the litigation the production of ephemeral data and name specific, relevant sources and locations. Otherwise, a court may find that the delay in seeking ephemeral data sources weighs against later compelling the producing party to collect, review, and produce that data (see, for example, *Milbeck*, 2019 WL 4570017, at *1-3 (noting statements in an expert affidavit indicating the time and burden that would be involved in converting, processing, and reviewing 1.67 gigabytes of compressed Slack data, which could yield as much as 17 million messages)).

Search Document Production Protocols in Federal Civil Litigation for more on how counsel may use a document production protocol to establish the parties' rights and obligations when producing documents and electronically stored information in discovery.

RAMIFICATIONS OF FAILING TO PRESERVE AND COLLECT EPHEMERAL DATA

FRCP 37(e) was amended in 2015 to clarify when a court may award sanctions for spoliation. Under this provision, a court may award sanctions only if relevant electronically stored information (ESI) is lost because a party failed to take reasonable steps to preserve the ESI and the party intended to deprive the requesting party of the information. Companies or individuals that were able to preserve ephemeral data or should have suspended routine use of ephemeral messaging tools upon notice or reasonable anticipation of litigation, but failed to do so, may be exposed to:

- An adverse inference presumption or jury instruction.
- A default judgment or dismissal.
- Monetary sanctions.

Similarly, parties who begin using ephemeral messaging applications or suddenly turn on auto-delete functions after a reasonable anticipation of litigation arises are also likely to face sanctions (see, for example, *Fed. Trade Comm'n v. Noland*, 2021 WL 3857413, at *1-4 (D. Ariz. Aug. 30, 2021) (imposing sanctions against defendants who, after they learned of a Federal Trade Commission investigation, installed an encrypted ephemeral messaging application to communicate about work-related items, turned on the auto-delete function, and ultimately deleted the application before turning over devices for forensic investigation)).

The issue of whether a spoliating party could have preserved ephemeral data or should have restricted use of the ephemeral messaging tool given the vanishing nature of the data is likely to be a point of contention in these contexts. However, where a company generated but did not retain ephemeral data before the duty to preserve was triggered, courts are not likely to make a finding of spoliation based on the company's failure to later produce that data in litigation (see, for example, *Williams*, 2020 WL 528604, at *2 (holding that the defendant had produced all known messages captured by screenshots and that no other messages remained in light of the instant messaging platform's construct); *King v. Catholic Health Initiatives*, 2019 WL 6699705, at *5 (D. Neb. Dec. 9, 2019) (denying a motion to compel Microsoft Lync instant messages and chats because those that had been saved to the company's systems had already been produced and other purportedly relevant messages were ephemeral and therefore not preserved due to the platform's settings)).

Search Sanctions for ESI Spoliation Under FRCP 37(e): Overview for more on sanctions for the failure to preserve ESI under FRCP 37(e), including the requirements for imposing sanctions and the types of sanctions that the rule permits.