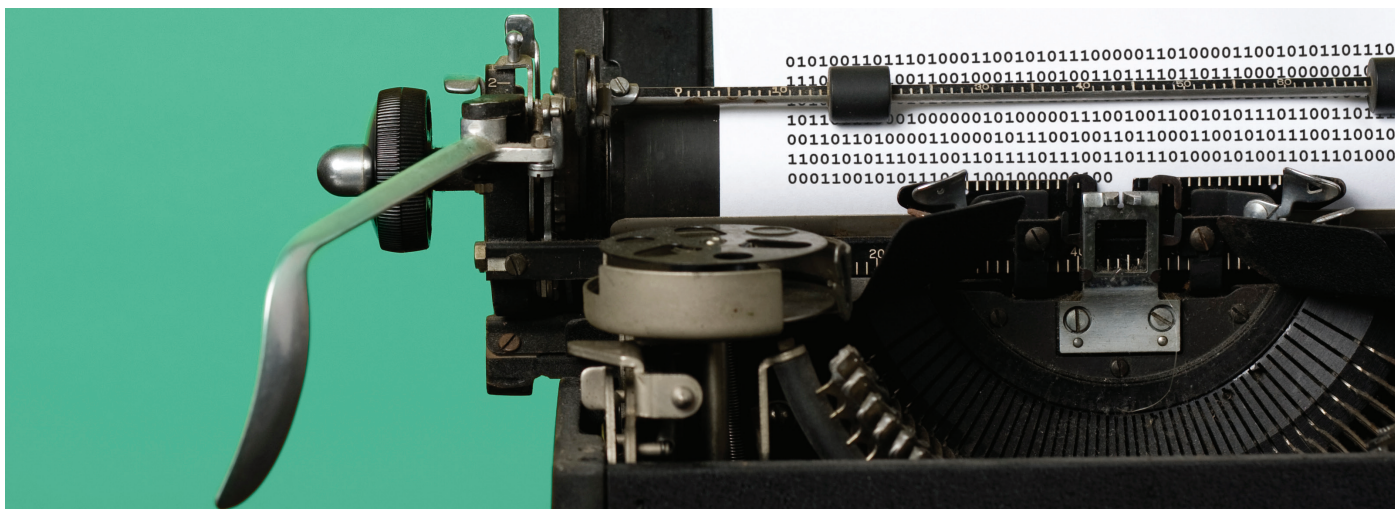


Ephemeral Messaging: Balancing the Benefits and Risks

Phil Favro





Ephemeral Messaging: Balancing the Benefits and Risks

Ephemeral messaging can offer useful functionality for organizations, including the ability to automate the disposition of content and assert more control over corporate information in employee communications. However, it also raises potential business, legal, and reputational risks. Before incorporating ephemeral messaging technology into a corporate network, organizations and their counsel should carefully evaluate the benefits and explore risk mitigation strategies.

**PHILIP FAVRO**

CONSULTANT
DRIVEN, INC.

Phil is a trusted advisor to organizations and law firms on issues relating to discovery and information governance. He is a nationally recognized thought leader and legal scholar, having published numerous articles in leading industry publications and academic journals. Phil actively contributes to Working Group 1 of The Sedona Conference, where he serves as a member of the Steering Committee. He has approximately 20 years of discovery experience and previously advised clients regarding complex business disputes and discovery issues in his former litigation practice.

The proliferating use of mobile messaging applications (apps) has generated significant attention in recent years. Ephemeral messaging, in particular, has grown in popularity because it enables users to automate the destruction of content shared with others. This technology offers organizations a more secure medium for confidential communications and an attractive option to potentially strengthen aspects of their information governance programs.

However, the unique features of ephemeral messaging also pose significant risks that counsel should not underestimate. From the challenges of battling negative perceptions of how this technology is being used to the issues that can arise when dealing with government regulators, litigation adversaries, and courts, ephemeral messaging may arguably create more problems than solutions for some organizations.

Before adopting ephemeral messaging, organizations and their counsel must first examine its merits and make an informed choice

about its use within the corporate environment. Indeed, employing ephemeral messaging technology without careful consideration could be fatal to organizations in certain regulated industries.

Against this backdrop, this article:

- Explains the key features of, and variations among, ephemeral messaging apps.
- Explores the potential benefits and risks of ephemeral messaging for business users.
- Offers risk mitigation strategies to help organizations effectively implement ephemeral messaging technology.

EPHEMERAL MESSAGING FUNCTIONALITY

Although some traditional messaging apps and email accounts can be individually configured to include automated destruction functionality, they generally do not have all the same features offered by ephemeral messaging apps. Moreover, ephemeral messaging apps do not offer a uniform set of features or functionality.

COMPARISON TO TRADITIONAL MESSAGING APPS

Ephemeral messaging enables users to exchange content and automatically discard that content from all devices (that is, both the sender's device and the recipient's device) within a period of time after a message is sent. These automated destruction features are typically more robust than those offered by traditional messaging apps, which limit the automated destruction functionality to messages on the user's own mobile device after a specified time period or when certain customized criteria are met.

For example, iMessage, the native messaging app for devices sold by Apple, Inc., enables the automated destruction of a message 30 days or one year after a user sends or receives the message. However, the automated destruction of an iMessage text does not impact messages sent or received on the devices of other parties to the communication, who unilaterally control the disposition of the content on their own devices.

VARIATION AMONG EPHEMERAL MESSAGING APPS

Ephemeral messaging apps (such as Confide, Telegram, and Wickr) generally allow a user to delete messages from both the user's own device and the devices of those who either sent or received the messages. The user's ability to customize message destruction settings varies, though, from one app to the next. For example:

- Some apps like Confide instantaneously destroy all content upon closing the message.
- Other apps like Wickr provide the user with enhanced control over the disposition of messages by allowing the user to:
 - set a time period (ranging from seconds to months) to retain the information before it is discarded; and
 - modify retention and destruction periods by sender or recipient.

Some apps also offer additional features, such as message encryption and prevention of screenshots, that enable users to better protect the confidentiality of their messages. The number of features may vary based on whether a user employs a consumer-grade tool or an enterprise version of the technology.

BENEFITS OF EPHEMERAL MESSAGING

Ephemeral messaging enables an organization to:

- Safeguard confidential communications and sensitive content.
- Decrease the amount of data that it stores and facilitate compliance with data minimization requirements.
- Strengthen information retention policies and objectives.
- Increase the efficiency of the discovery process in litigation.

CONFIDENTIALITY

Ephemeral messaging developers often emphasize the confidentiality their technology affords over traditional messaging apps. Specifically, they spotlight how their apps:

- **Facilitate communication without retaining a record of every digital exchange.** Promoted as the digital equivalent of a water cooler discussion or a phone call, ephemeral messaging's automated destruction functionality allows users to communicate without concern that the content will be retained on users' devices indefinitely.
- **Protect against data security risks.** Developers highlight the tools' encryption of data that is at rest in the app, as well as data that is in transit between a sender and a recipient within the app. These measures are designed to provide users with a secure medium to discuss confidential topics while reducing the potential that content may be intercepted or replicated by cyber criminals or government regulators (see below *Scrutiny from Government Regulators*).

DATA MINIMIZATION

Ephemeral messaging may help organizations lower their data breach risks and address their obligations under various data protection laws by decreasing the amount of data they store. To satisfy data minimization requirements, organizations must closely examine the types and amounts of personal information they collect, use, and retain. The European Union (EU) General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is the most prominent of the laws addressing data minimization.

The GDPR generally requires that data controllers and processors minimize the personal information they maintain regarding consumers, employees, or others in the EU (GDPR, Article 5.1(c)). This mandate requires organizations to examine computer systems and upgrade to enhanced technologies that facilitate data minimization within the corporate network (GDPR, Article 25.1). In this regard, ephemeral messaging technologies — which curb the proliferation of communications stored on the corporate network — may be viewed as a means of compliance with the GDPR's data minimization directive.



Search [Overview of EU General Data Protection Regulation](#) for more on the GDPR.

INFORMATION RETENTION

Organizations can employ enterprise-grade ephemeral messaging tools to help implement their information retention programs. Specifically, an organization can use these tools to:

- **Customize retention periods.** Ephemeral messaging tools can schedule the automated destruction of messages to coincide with the time the retention program has established for maintaining communications.
- **Disable message destruction by individual employees.** Some enterprise-grade tools have a central archiving functionality that organizations can use to routinely (and automatically) preserve message content on a user-specific basis.



Search [Records Management Toolkit](#) for a collection of resources to help in-house counsel and law firm attorneys manage an organization's records and other data.

DISCOVERY

Ephemeral messaging may facilitate the efficiency of the discovery process in litigation. By reducing the number of messages maintained on employee devices, organizations can also decrease the amount of information that must be imaged or otherwise collected. This can potentially expedite the preservation and collection process and reduce discovery costs.

RISKS OF EPHEMERAL MESSAGING

While ephemeral messaging technology offers significant upside for business users, organizations should recognize that using these apps also presents several risks, including:

- The appearance of impropriety.
- Scrutiny from government regulators.
- The potential failure to satisfy common law preservation obligations.
- Possible tension with an organization's overall information governance strategy.
- Technological limitations and security issues.

Before implementing an ephemeral messaging program, organizations and their counsel should evaluate the nature and extent of these risks, which are more pronounced in certain regulated industries and for organizations with cross-border operations.

APPEARANCE OF IMPROPRIETY

Organizations must consider the common perception that ephemeral messaging is used for nefarious purposes. Because ephemeral messaging apps automate the destruction of messages, many perceive — rightly or wrongly — that users employ the technology to hide evidence of wrongdoing.

Indeed, the mere use of ephemeral messaging could arguably create an appearance of impropriety. This is evident from news coverage of the apparently unauthorized use of ephemeral messaging by politicians, government employees, and law enforcement officials in recent years. For example, former Missouri governor Eric Greitens faced controversy over his use of Confide for government business. Additionally, the City of Long Beach, California suspended the use of the app TigerText after stories surfaced that police officers were communicating through the app to prevent discovery of their discussions.

Organizations that use ephemeral messaging tools for legitimate business purposes could still face skepticism or backlash from various groups, including:

- Government regulators or adverse parties and judges in litigation, who may assert that ephemeral messaging apps were used to conceal evidence of wrongdoing.
- Investors (in the case of publicly traded companies), who may believe the use of ephemeral messaging apps could damage the corporate brand or otherwise lower the value of their investment.

SCRUTINY FROM GOVERNMENT REGULATORS

Even the most measured approach to ephemeral messaging may not alleviate concerns held by government regulators, such as the Securities and Exchange Commission (SEC) and the Department of Justice (DOJ).

SEC

The SEC recommends that investment advisers not use ephemeral messaging if they wish to comply with the “books and records rule” in the Investment Advisers Act of 1940. This rule requires investment advisers to make and keep certain books and records related to their investment advisory business (17 C.F.R. § 275.204-2).

The SEC's National Office of Compliance Inspections and Examinations (OCIE) recently published a risk alert stating that advisers should “[s]pecifically 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” (OCIE Risk Alert, Observations from Investment Adviser Examinations Relating to Electronic Messaging (Dec. 14, 2018), available at [sec.gov](#)).

This prohibition on ephemeral messaging is not surprising given the overall recordkeeping mandate under the Securities Exchange Act of 1934. That directive requires a broker or dealer to keep communications “relating to its business as such” for at least three years (17 C.F.R. § 240.17a-4(b)(4)). The Financial Industry Regulatory Authority (FINRA) has clarified that the recordkeeping rule specifically applies to text messaging apps and chat services (FINRA Regulatory Notice 17-18, Social Media and Digital Communications: Guidance on Social Networking Websites and Business Communications (Apr. 2017), available at [finra.org](#)). Although FINRA's guidance does not specifically refer

to ephemeral messaging, organizations should probably avoid adopting an ephemeral messaging program given this clear regulatory opposition.

DOJ

The DOJ has also expressed skepticism toward ephemeral messaging. In 2017, the DOJ's Foreign Corrupt Practices Act (FCPA) enforcement division published guidance indicating that organizations being investigated for FCPA violations could obtain cooperation credit only if they forbade their employees from using ephemeral messaging (DOJ, US Attorneys' Manual Insert 9-47.120 – FCPA Corporate Enforcement Policy (Nov. 29, 2017), available at [justice.gov](https://www.justice.gov)).

However, in the face of criticism from affected organizations using ephemeral messaging for legitimate business purposes, the DOJ modified its FCPA corporate enforcement policy in March 2019. Organizations may now use ephemeral messaging as long as they have safeguards that ensure communications and other documents are retained pursuant to a corporate information retention policy or applicable legal requirements (DOJ, Justice Manual 9-47.120(3)(c) – FCPA Corporate Enforcement Policy, available at [justice.gov](https://www.justice.gov)).

By acknowledging that organizations may use ephemeral messaging in connection with an information retention program, the DOJ's revised policy:

- Appears to strike a reasonable balance between the DOJ's investigation needs and reasonable corporate imperatives for information governance (though some attorneys have questioned whether the revised policy has made a difference in practice).
- Is more consistent with US case law, which recognizes that organizations may implement neutral retention policies to eliminate documents that are not subject to a preservation obligation (see, for example, *Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 (2005); *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1322 (Fed. Cir. 2011) (approving corporate retention policies that are adopted for "good housekeeping" purposes)). Indeed, the US Supreme Court has conceded that corporate retention policies adopted for legitimate purposes may be valid even if they are designed to keep documents from the government (*Arthur Anderson*, 544 U.S. at 704).



Search [The Foreign Corrupt Practices Act: Overview](#) for more on FCPA compliance.

Search [Criminal and Civil Liability for Corporations, Officers, and Directors](#) for more on receiving cooperation credit in government investigations.

FAILURE TO SATISFY PRESERVATION OBLIGATIONS

Organizations have a common law obligation to preserve relevant evidence when litigation is pending or reasonably anticipated (2015 Advisory Committee's Note to FRCP 37(e)). This directive generally requires organizations to suspend ordinary retention practices that might otherwise eliminate relevant documents. The failure to do so may result in sanctions

(FRCP 37(e); see *Paisley Park Enters., Inc. v. Boxill*, 2019 WL 1036058, at *4, *7-8 (D. Minn. Mar. 5, 2019) (imposing sanctions for evidence destruction that resulted when the defendants failed to disable the auto-delete function affecting retention of text messages on their mobile phones)).

Organizations that use ephemeral messaging face the risk of potential destruction of information that might otherwise be used as evidence in litigation. Although some ephemeral messaging apps allow users to modify their settings and keep relevant messages, thereby satisfying the duty to preserve, many do not. For example, Confide instantaneously deletes content, including any record that a communication even transpired (such as the date of the message and the parties who exchanged it).

The recent decision in *Waymo LLC v. Uber Technologies, Inc.* demonstrates how ephemeral messaging can deprive adversaries of relevant evidence in litigation. *Waymo* involved a high-stakes trade secret dispute over autonomous vehicle technology. *Waymo* accused Uber of using Wickr and Telegram to eliminate relevant evidence before it could be preserved and produced in discovery. Despite extensive testimony and other evidence regarding Uber's use of ephemeral messaging, the court did not find that Uber used the technology to intentionally destroy relevant information. Nevertheless, the court allowed *Waymo* to present evidence and argument to the jury that Uber's use of ephemeral messaging created "gaps in *Waymo*'s proof that Uber misappropriated trade secrets." In turn, Uber was permitted to present evidence and argument regarding its legitimate business use of ephemeral messaging. (2018 WL 646701, at *3, *18, *21 (N.D. Cal. Jan. 30, 2018).)



Search [Sanctions for ESI Spoliation Under FRCP 37\(e\): Overview](#) for more on sanctions for loss or destruction of evidence.

Search [Litigation Hold Toolkit](#) for a collection of resources to help counsel preserve documents and implement a legal hold.

TENSION WITH INFORMATION GOVERNANCE STRATEGY

Information governance is premised on the transparency of the information that an organization generates, receives, and maintains. This can stand at odds with the automated destruction and confidentiality features of ephemeral messaging. Key functions of an information governance program include:

- Mapping the organization's data.
- Monitoring the organization's information systems.
- Conducting audits to ensure compliance with policies and procedures relating to the use of information.
- Implementing legal holds to address discovery demands for information in response to litigation and investigations.

Unless ephemeral messaging is deployed under the aegis of a robust information governance program, it could create perilous conditions in the corporate environment. The risks are particularly acute where employees use unapproved or forbidden consumer-grade tools. Some potential risks include:

- Failing to detect corruption.
- Facilitating the misappropriation of confidential or sensitive information.
- Undermining information retention policies and other compliance initiatives.



Search [Information Governance: Establishing a Program and Executing Initial Projects](#) for more on developing and implementing an information governance program.

TECHNOLOGICAL LIMITATIONS AND SECURITY ISSUES

Organizations should evaluate whether an app's technology features actually live up to the claims reflected in the developer's marketing literature. While the developer may tout the ephemeral nature of its messages, not every technology is as robust as its promotional materials suggest (see, for example, Electronic Frontier Foundation, *Between You, Me, and Google: Problems with Gmail's "Confidential Mode"* (July 20, 2018) (describing various limitations of Gmail's Confidential Mode ephemeral technology), available at eff.org).

The cautionary tale of the popular app Snapchat is particularly instructive on this issue. Snapchat previously touted certain ephemerality features of its messaging technology by:

- Claiming that messages transmitted through its app (including those with images and video) would "disappear forever" after a certain time period.
- Highlighting the ability of its technology to prevent screenshots by message recipients.

Both of these claims turned out to be false, leading to a Federal Trade Commission (FTC) complaint and a settlement of the FTC charges (see Press Release, *Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False* (May 8, 2014), available at ftc.gov).

While the Snapchat debacle involved consumers, its lessons are equally applicable in the corporate context. Not every ephemeral messaging technology will include the confidentiality, automated destruction, and customization features that companies likely need to satisfy their business objectives. Nor is every technology enterprise grade. Carefully reviewing a technology's offerings is advisable before acquisition and deployment in the organization.

RISK MITIGATION STRATEGIES

To minimize the various risks associated with ephemeral messaging, organizations and their counsel should carefully review and take steps to enhance their information governance policies and practices, and examine the particular technology they seek to use. For example, an organization should:

- **Develop a written policy that delineates the organization's use case for ephemeral messaging.** To deal with skepticism or backlash from regulators, judges, or others who may distrust the use of ephemeral messaging, an organization should have a written policy that:

- sets out the organization's legitimate business needs for the ephemeral messaging tools;
- addresses the benefits and risks of the ephemeral messaging technology;
- identifies risk mitigation strategies that the organization has implemented; and
- supports and is consistent with the organization's existing information-related policies and procedures.

- **Design an internal compliance program tailored to the organization's ephemeral messaging platforms and use.**

An organization can help ease regulators' concerns and demonstrate the reasonable use of ephemeral messaging by developing an internal compliance program. Such a program will ideally be a top-down, neutral process that is well-integrated with the organization's information governance program. Coupling that process with an ephemeral messaging technology that offers a central archiving feature will only serve to bolster the efficacy of the compliance program. These measures are probably essential for organizations hoping to satisfy the DOJ's cooperation credit requirements for FCPA violations. They may also be helpful if the organization's ephemeral messaging use is challenged in litigation (see *Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1193-94 (D. Utah 2009) (discussing the importance of substantiating the reasonableness of a corporate information retention policy)).

- **Implement a mobile device use policy that specifically addresses ephemeral messaging.** Regardless of whether an organization issues computers and mobile devices to employees or has a "bring your own device" (BYOD) environment, the organization should ensure it incorporates into its information governance program a robust mobile device use policy that addresses the use of unapproved or consumer-grade ephemeral messaging tools. Additionally, the organization should:

- conduct employee training and policy audits; and
- actively enforce the policy and discipline employees for noncompliance.

- **Be aware of the preservation limitations of certain ephemeral messaging tools.** To avoid a discovery sanction or the protracted motion practice that plagued Uber in the *Waymo* litigation, an organization should ensure the ephemeral messaging technology it implements has legal hold functionality. That functionality should allow the organization to simultaneously:

- place custodians of relevant information on hold; and
- continue to automate the destruction of other non-relevant communications.