Published on *The National Law Review* https://natlawreview.com

Disappearing Messages, Unofficial Communications Platforms and Ever-Increasing Scrutiny by Regulators

Article By:

Michelle A. Freeman

Corporate use of third-party messaging platforms, including ephemeral messaging tools (which allow messages to disappear), is quite common and has become both a cost efficiency for employers and a convenient way for employees to communicate quickly with colleagues and clients. However, regulators are increasingly concerned that companies are not doing enough to preserve and produce communications from messaging platforms relevant to government investigations, litigation, or other legal processes.

In recent months, federal regulators warned that companies may be subject to criminal prosecution if they fail to adequately retain and produce this type of data. In January 2024, the Department of Justice (DOJ) and Federal Trade Commission (FTC) announced that they were updating the language in their standard preservation letters, subpoenas, and second requests to make explicitly clear that a company's (and its counsel's) legal responsibility to preserve evidence extends to new methods of communications, such as collaboration and information sharing tools and ephemeral messaging. This means that, once the obligation to preserve is triggered, companies will need to quickly locate any relevant messages on platforms, such as Slack, Microsoft Teams, Zoom, Google Chat, Zoom, Snapchat, WhatsApp, Telegram, and Signal.

The announcement quoted Manish Kumar, Deputy Assistant Attorney General of the Justice Department's Antitrust Division: regulators "expect that opposing counsel will preserve and produce any and all responsive documents, including data from ephemeral messaging applications designed to hide evidence. Failure to produce such documents may result in obstruction of justice charges."

What Are Ephemeral Messages?

Pure ephemeral messages are self-destructing messages with no backup or archiving option. Unlike a typical text message that is sent and remains on a user's and receiver's phone until manually deleted, ephemeral messages delete themselves after a set time. Some examples of platforms that offer this type of feature are Signal, WhatsApp, WeChat, and Snapchat.

Platforms utilize different features which can impact the degree a message is ephemeral. The following chart outlines different types of ephemeral messaging and their defining characteristics.

Ephemeral Messaging	Messages are automatically deleted upon review. No message storage ability. Messages are encrypted in a way that message content is generally inaccessible.
Quasi-Ephemeral Messaging	User has some control over message deletion settings.Messages may have the ability to be forwarded or saved in some way. Deleted messages are still accessible in some form via metadata. Companies that purchase licenses/subscriptions for employees to access these platforms can often control the retention settings.
Non-Ephemeral Messaging	Automated message deletion is not a key feature of the platform.Message deletion is not reciprocal. (If the sender deletes a message they sent, it is not deleted on the receiver's side.)Messages are generally not encrypted.

The DOJ has acknowledged that there are legitimate reasons to use messaging platforms with ephemeral features, as these features increase security and decrease data clutter. But these benefits do not come without risks. Even typical workplace messaging platforms such as Slack and Microsoft Teams, which have ephemeral components, can create liability issues for a company. These risks are amplified when companies allow employees to use unofficial messaging platforms or personal devices without a strategy in place to quickly locate and preserve data when required.

How Can Companies Respond to the Increased Scrutiny?

Federal regulators are moving beyond simply reviewing a company's official compliance program and will consider how employees actually use messaging platforms for business communications. As a result, companies should understand how and why employee communications vary by business function and jurisdiction, as well as the policies in place to preserve and manage messaging platforms, including whether employees have control over any retention settings.

If your company cannot adequately answer these questions, it may be time to reassess your compliance policies and controls:

- Assess your company's use of encrypted, ephemeral, and unofficial message platforms and determine your company's risk profile based on the DOJ's recently updated guidance for corporate compliance programs.
- Review your company's licensed messaging platforms to identify options for preserving data and consider restricting the use of any platforms where ephemeral messages cannot be retained if investigations or legal proceedings are threatened.
- Evaluate your company's corporate compliance program and any "bring your own device" (BYOD) policy and revise as necessary to ensure the policies adequately address encrypted, ephemeral, and unofficial messaging platforms.
- Update legal holds and related preservation procedures to be in line with the relevant regulatory guidance.

- Provide education and training to employees regarding company policies on ephemeral messaging and personal devices or unofficial messaging platforms, and monitor employee compliance.

These are complicated issues which require tailored solutions and the balancing of competing interests. As the technology continues to evolve, companies will need to consider whether additional steps can or should be taken to limit future liability.

National Law Review, Volume XIV, Number 281