Cooley

DOJ Issues Further Guidance, Warnings on Ephemeral Messaging Apps

March 21, 2023

At the March 2023 American Bar Association National Institute on White Collar Crime, senior Department of Justice officials offered their most expansive guidance yet about the dangers of using ephemeral messaging for company communications. Officials noted that when conducting an investigation, DOJ prosecutors will consider a company's use of ephemeral and encrypted applications, whether the company preserved those communications, and if those messages are accessible for the investigation, as well as company policies governing such apps. And they warned in no uncertain terms that if a company does not turn over these types of communications, "prosecutors will not accept that at face value ." Where a company fails to produce such communications, prosecutors will further scrutinize the company's ability to access those communications and how they are stored, among other things. Officials made clear that " company's answers – or lack of answers – may very well affect the offer it receives to resolve criminal liability."

The DOJ's most recent comments follow a memorandum from September 2022 recommending that companies institute compensation clawback measures to ensure employees adhere to corporate compliance policies, including policies governing employee use of personal devices and third-party messaging apps such as Signal, Telegram, WhatsApp, etc. The memo noted that corporations with robust compliance should have these types of device and messaging policies, provide training to employees on them, and enforce the policies when violations are identified. It also cautioned that "ow companies address the use of personal devices and third-party messaging platforms can impact a prosecutor's evaluation of the effectiveness of a corporation's compliance program, as well as the assessment of a corporation's cooperation during a criminal investigation." Additional DOJ guidance provided in December 2022 zeroed in on encrypted and ephemeral messaging apps, observing that while there may be legitimate uses for those tools for company business, they can present significant challenges to a company's ability to ensure it has a well-functioning compliance program, and more importantly, the ability to access those communications when required. The DOJ's guidance on messaging apps comes against the backdrop of a renewed focus on corporate enforcement and vigilance against corporate malfeasance.

As early as 2017, the DOJ's Foreign Corrupt Practices Act (FCPA) enforcement division had published guidance that organizations being investigated for FCPA violations could obtain a cooperation credit only if they disallowed the use of ephemeral messaging by employees. However, noting that many organizations use ephemeral messaging for legitimate business reasons, it later softened its stance, instead requiring organizations using ephemeral apps to have safeguards to ensure information is retained pursuant to retention policies and legal requirements.

What is ephemeral messaging?

Ephemeral messaging apps are communication platforms that automatically erase the conversation between parties immediately or after a short amount of time. Automatic deletion can be the application's default or a feature that users or administrators can turn on and off. While ephemeral messaging has several real-world benefits, including privacy and security, it can be problematic for businesses that need to preserve information for regulatory, compliance, litigation or legal holds, or other reasons. Similar communication mediums such as text messages, in-application chat features and direct messages in social media accounts can prove equally problematic due to their decentralized nature, with the messages often residing on users' devices or accounts beyond the reach of company controls. Other issues can arise when messaging apps are used to further illegal or disfavored activities by way of eliminating incriminating conversations or evidence of wrongdoing. Courts and regulatory agencies such as the DOJ have taken notice, cautioning organizations on the potential hazards of using messaging apps for business activities without sufficient policies and procedures in place to monitor compliance and preserve communications when necessary.

Actions against broker-dealers and investment advisers

In September 2022, the Securities and Exchange Commission and the Commodity Futures Trading Commission (CFTC) reached a combined $1.8 billion settlement with 15 broker-dealers and an investment adviser related to a failure to preserve electronic communications. Regulators focused on the widespread use of what the SEC called "off-channel" messaging communications, in particular text messages and messaging apps, that were not preserved as required of

broker-dealers and investment advisers by SEC and CFTC record-keeping regulations. In December 2021, the SEC announced a $125 million fine against a large financial institution related to failures to preserve staff communications on personal mobile devices and messaging applications.

The SEC highlighted concerns related to ephemeral messaging in a Risk Alert issued in December 2018 reminding registered investment advisers of their retention obligations pursuant to SEC rules.[1] Noting an increase in the use of text messaging or chat apps to communicate, the SEC recommended that advisers review their policies and processes related to electronic messaging to ensure compliance with retention rules. In October 2021, SEC Division of Enforcement Director Gurbir Grewal indicated that companies "need to be actively thinking about and addressing the many compliance issues raised by the increased use of personal devices, new communications channels, and other technological developments like ephemeral apps."

Litigation pitfalls

Ephemeral apps and text messages also have proven to pose issues for judges and parties in litigation, particularly in the context of preservation obligations in discovery. In *Herzig v. Arkansas Foundation for Medical Care, Inc.*,[2] the defendant alleged that the plaintiffs decided to install and use the ephemeral messaging application Signal to intentionally destroy discoverable evidence, despite the fact that they were subject to legal holds. The court found that the Signal communications were most likely responsive and that the plaintiffs' decision to use Signal was done in bad faith.

Organizations that do not have controls or effective legal hold policies in place also run the risk of increased costs as the focus of the case shifts away from the merits to expensive discovery disputes that could result in case-ending sanctions.

Minimizing legal and compliance risks

It is imperative that companies have enforceable policies and controls in place to minimize legal and compliance risks from employee use of ephemeral messaging apps. Below, we've summarized actions companies can take.

Retention program and information policies

Create and implement practical retention policies for electronic messaging apps that are authorized by the company, and ensure compliance with applicable rules and regulations. This includes monitoring compliance and addressing noncompliant use of prohibited applications for business purposes. These policies also need to harmonize with the organization's acceptable use policies for technology – and clearly define business communications and messaging guidelines.

Mobile devices and applications

Design functional mobile device policies and administer mobile device management software to manage apps on devices used for business purposes, including personal devices.

Legal holds

Establish proactive legal hold response procedures to prepare for potential litigation or regulatory activity.

Training and oversight

Develop training programs to educate employees regarding company policies and permissible communication applications, as well as apps prohibited for business purposes. Empower employees to understand their role in helping the company manage risk.

Next steps

Cooley can assist you in creating practical and effective information, device, and electronic messaging policies, and we can guide you through the implementation, administration and oversight process. We also can help your company design and implement defensible legal hold processes and procedures to navigate the complexities of the eDiscovery process. For more information, please reach out to one of the lawyers listed below.

Notes

1. Advisers Act Rule 204-2, which is also known as the “Books and Records Rule,” requires advisers to make and keep certain books and records relating to their investment advisory business, including typical accounting and other business records as required by the SEC.
2. No. 2:18-CV-02101, 2019 WL 2870106 (W.D. Ark., July 3, 2019).

Contributors

Luke Cadigan
Bio

Michelle Galloway
Bio

Andrew Goldstein
Bio

Ruth Hauswirth
Bio

Matthew Krengel
Bio
