Cooley

Federal Law Enforcement Recommends Encrypted and Ephemeral Messaging

January 15, 2025

In light of recent reports of cyberattacks on telecommunications companies, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) issued a series of reports and statements recommending secure communications, including using end-to-end encryption. At the same time, US regulators – including the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) – have taken an increasingly aggressive approach to discourage companies from utilizing encrypted and ephemeral messaging platforms. The federal government's inconsistent stances on these technologies create inherent tensions for companies and raise the question of whether regulators will revise their guidance, or whether companies will be forced to choose between secure communications and regulatory compliance.

FBI and CISA recommend using encrypted and ephemeral messaging

On a December 3, 2024 call with the press, FBI and CISA officials warned against unencrypted text and voice communications. Jeff Greene, CISA's executive assistant director for cybersecurity, stated, "Encryption is your friend, whether it's on text messaging or if you have the capacity to use encrypted voice communication. Even if the adversary is able to intercept the data, if it is encrypted, it will make it impossible, if not really hard, for them to detect it." The next day, the FBI, CISA, and several other US and foreign agencies released guidance for strengthening network devices against potential exploitation. Among other things, the guidance recommends network engineers to "ensure that traffic is end-to-end encrypted to the maximum extent possible."

Two weeks later, on December 18, 2024, CISA published Mobile Communications Best Practice Guidance, which aims to "promote protections for mobile communications from exploitation" by cyberattacks. The guidance is directed at "highly targeted" senior government officials and senior politicians, though CISA notes that it is "applicable to all audiences." CISA's guidance makes general recommendations for devices and online accounts, as well as specific recommendations for iPhone and Android users.

Topping the list of CISA's general recommendations is to "**use only end-to-end encrypted communications**." CISA recommends individuals to "adopt a free messaging application for secure communications that guarantees end-to-end encryption, **such as Signal or similar apps**." To ensure that messages between different operating systems (e.g., iPhones and Androids) remain secure, CISA also recommends using a messaging app that is compatible with both systems. CISA notes that such apps "**may include features like disappearing messages and images, which can enhance privacy**."

Other general recommendations include:

- Enabling Fast Identity Online (FIDO) phishing-resistant authentication
- Migrating away from Short Message Service (SMS)-based multifactor authentication (due to the fact that SMS messages are not encrypted)
- Using a password manager
- Setting a Telco PIN (offered by most telecommunications providers)
- Regularly updating software
- Opting for the latest hardware version from the cell phone manufacturer
- Not using a personal virtual private network (VPN)

With respect to iPhone users, CISA recommends enabling Lockdown Mode, disabling certain settings to ensure that messages do not send as SMS if iMessage is unavailable, and using encrypted Domain Name System (DNS) services, among other things.

As for Android users, CISA recommends using phones from manufacturers with strong security track records, using only

Rich Communication Services if end-to-end encryption is enabled, and using encrypted DNS services, among other things.

Regulators warn of noncompliance risks regarding encrypted and ephemeral messaging

As we reported in March 2024, over the past several years, US regulators have increasingly focused on corporate use of ephemeral and encrypted messaging due to the challenges of retrieving and reviewing such communications at a later date. DOJ officials have stated that when conducting an investigation, prosecutors will consider a company's use of ephemeral and encrypted applications, whether the company preserved those communications and whether those messages are accessible for the investigation. Failure to produce such communications may adversely impact the offer that a company receives to resolve criminal liability.

The DOJ's most recent version of Evaluation of Corporate Compliance Programs reinforces this stance, noting that prosecutors will consider a corporation's policies and procedures governing the use of communications platforms, including ephemeral messaging applications. In a January 2024 joint press release with the Federal Trade Commission (FTC) regarding the agencies' updated standard preservation letters and specifications for second requests, the agencies specifically called out the ephemeral messaging application Signal as one of the messaging platforms that allows "immediate and irretrievable destruction of communications and documents," and warned companies that failure to preserve data from ephemeral messaging platforms will be treated as spoliation or even obstruction of justice.

In addition, as we reported in December 2024, since 2021, the SEC has conducted a broad sweep of financial institutions, focusing on whether employees communicated about business matters over text messages or other messaging apps. In particular, the SEC looks to whether a company's employees use ephemeral and encrypted messages that make it difficult for the company to monitor and preserve communications. The SEC's "off-channel communications" sweep has resulted in charges against more than 100 firms, with more than $2 billion in penalties levied, including $63.1 million in penalties against 12 firms from earlier this week. A similar sweep by the Commodity Futures Trading Commission (CFTC) resulted in more than $1.23 billion in civil monetary penalties imposed against 28 financial institutions.

Both SEC Chair Gary Gensler and CFTC Chair Rostin Behnam have announced that they plan to depart on January 20, 2025. There is early indication that their successors (to be appointed by incoming President Donald Trump) may roll back the off-channel communications sweep. In September 2024, the Republican SEC commissioners issued a statement urging their colleagues to "reconsider current approach to the off-channel communications issue." In the statement, Commissioner Hester Peirce and Commissioner Mark Uyeda noted that "it does not appear that firms have an achievable path to compliance," and that the SEC's current approach "equates reasonableness with perfection." The commissioners recommended "work with the industry" and taking a more "privacy-respecting approach."

The FBI's and CISA's recent advisories indicate the agencies' recognition that companies have legitimate needs for using encryption and ephemeral messaging to protect sensitive business communications. CISA's guidance specifically recommends using Signal because it "guarantees end-to-end encryption." It remains to be seen whether these agencies' view on encryption and ephemeral messaging signals a policy shift in the federal government that will be reflected in subsequent policy changes at the DOJ and SEC, or whether companies will be forced to choose between the necessity of secure communications for sensitive business discussions and the demand for regulatory compliance and cooperation in government investigations.

Contributors

Andrew Goldstein
Bio

Daniel Grooms
Bio

Bingxin Wu
Bio
