

Encrypted Electronic Instant Messaging Applications Continue to Catch the Government's Attention

WRITTEN BY

Casselle A.E. Smith | Ghillaine A. Reid | Jay A. Dubow | Tomi Balogun

In March 2023, the Department of Justice (DOJ) Criminal Division updated its [Evaluation of Corporate Compliance Programs \(ECCP\)](#) guidance to address the use of personal devices and third-party messaging applications by corporate employees. Assistant Attorney General Polite announced the new guidance during his speech at the ABA's *38th Annual National Institute on White Collar Crime Conference*. It follows Deputy Attorney General Monaco's September 2022 directive that the Criminal Division study best corporate practices regarding messaging and incorporate them into the next edition of the ECCP.

First issued in 2017 and last updated in 2020, the ECCP helps prosecutors assess the effectiveness of a corporation's compliance program and sets forth factors to be considered when determining whether and how to resolve investigations of corporate misconduct. In connection with that analysis, prosecutors now must consider whether a corporation has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms — including ephemeral applications, such as WhatsApp and Signal. Federal prosecutors will look for data preservation mechanisms that allow companies to identify, investigate, report, and remediate employee misconduct and legal violations. Companies that lack policies regarding employees' work-related use of personal cellphones and messaging apps should expect steeper penalties for misconduct.

The Criminal Division did not suggest a one-size-fits-all approach. Rather, the ECCP notes that relevant policies should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company. Companies in heavily regulated industries — particularly financial institutions — should expect a greater degree of scrutiny, as their failure to preserve all business-related communications for a period of years may itself violate the law. As noted in [our August 2022 client alert](#), the Securities and Exchange Commission (SEC) has cracked down on encrypted and other off-platform communications by senior Wall Street executives at the nation's major investment banks. In a record-setting \$200 million settlement, the SEC and the Commodity Futures Trading Commission (CFTC) jointly settled enforcement actions with a Wall Street firm for failing to adequately monitor employee communications and circumventing recordkeeping requirements. This investigation centered around the firm's failure to monitor business-related communications on platforms like WhatsApp, resulting in a combined settlement of \$200 million in penalties.

As highlighted in the DOJ memo, companies should take decisive and effective action to enhance their policies and procedures, as well as how they design their compliance program on the use of personal devices and third-party messaging apps. Companies will benefit from strong and efficient procedures, including an ability to conduct seamless internal investigations, ensure business continuity when an employee departs, and an ability to gather

business communication relevant to litigation. Companies that fail to do so will be susceptible to regulators' crack down for lack of sufficient compliance and internal controls.

In light of this recent DOJ memo and SEC enforcement initiatives, members of Troutman Pepper's Securities Investigations + Enforcement group, in coordination with eMerge, the firm's eDiscovery and data management subsidiary, are available to provide further guidance, including conducting internal reviews of messaging and communication retention rules and procedures, developing strong and effective policies and procedures that will aid retention and preservation of business-related communications, and most importantly, advising on how to effectively and consistently effect these policies and procedures.

RELATED INDUSTRIES + PRACTICES

- [Securities Investigations + Enforcement](#)
- [Securities Litigation](#)
- [White Collar Litigation + Investigations](#)
- [eDiscovery + Data Management](#)