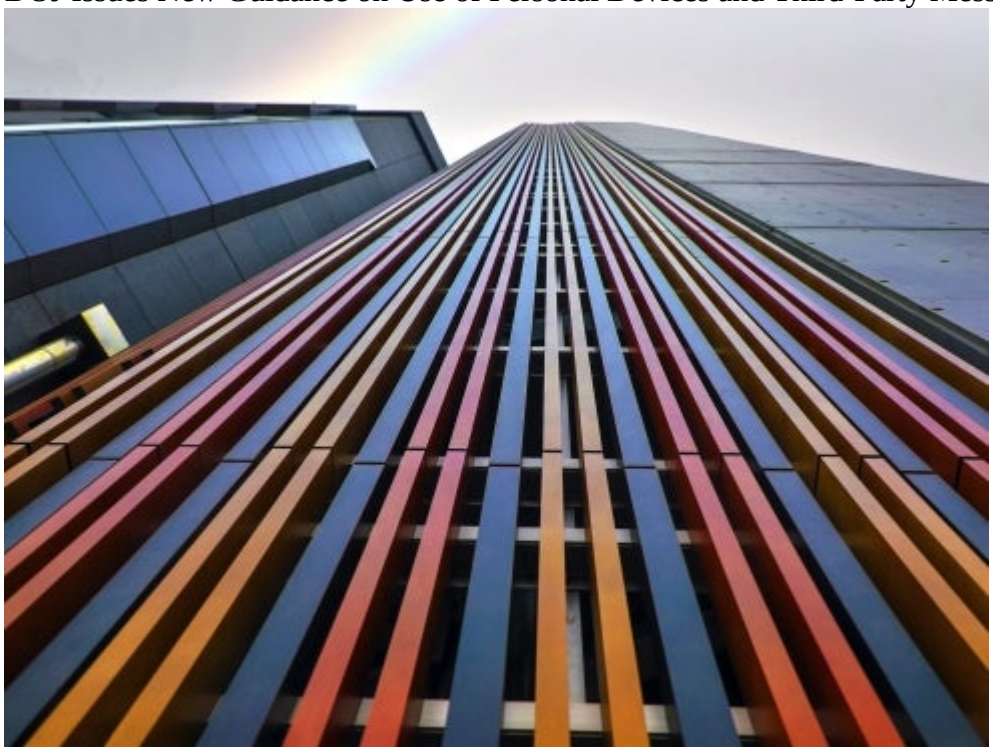
Updates
March 16, 2023
DOJ Issues New Guidance on Use of Personal Devices and Third-Party Messaging Applications



The U.S. Department of Justice (DOJ) announced significant new guidance on March 3, 2023, regarding the use of personal devices and the retention of corporate communications. The DOJ's concern regarding the use of personal devices and third-party messaging applications has been growing for years, as these applications have increasingly contributed to preservation issues that have impeded DOJ (and internal) investigations.

This announcement expands on a prior memorandum issued by the DOJ in September 2022, which advised that "all corporations with robust compliance programs should have effective policies governing the use of personal devices and third-party messaging platforms for corporate communications." (More information on this prior memorandum is available here and here.) At that time, the DOJ promised to update its corporate compliance guidance to provide more detail as to the agency's expectations. In keeping with that commitment, the DOJ has provided revised guidance on the Evaluation of Corporate Compliance Programs (ECCP), under which prosecutors are now explicitly instructed to "consider a corporation's approach to the use of personal devices as well as various communications platforms and messaging applications, including those offering ephemeral messaging."

During remarks at the American Bar Association's (ABA) recent National Institute on White Collar Crime, Assistant Attorney General Kenneth Polite, Jr. explained that, under the revised ECCP, a corporation's communications and messaging policies "should be tailored to the corporation's risk profile and specific business needs" and should "ensure that, as appropriate, business-related electronic data and communications can be preserved and accessed." Polite added that a corporation's approach to this issue "*may very well affect the offer it receives to resolve criminal liability*." (Emphasis added.)

The revised ECCP, and Polite's accompanying statement, further underscore the importance of companies' developing and effectively implementing clear written policies regarding the preservation of all business-related communications, including text messages and messages sent using ephemeral messing applications, as well as business-related messages sent from personal devices. A company's failure to do so could result in significant

adverse consequences in the event of a DOJ investigation or enforcement action.

Revisions to the ECCP

The revised ECCP makes clear that the DOJ expects effective compliance programs to include policies governing the acceptable use of personal and corporate devices and data preservation in relation to such devices. The guidance directs prosecutors considering the appropriateness of any corporate compliance program to evaluate (1) how such policies are communicated to employees and (2) whether they have been enforced "on a regular and consistent basis in practice."

Importantly, the DOJ acknowledges that there is no one-size-fits-all solution to preserving business-related electronic data. Rather, the revised ECCP notes that "[p]olicies governing such applications should be tailored to the corporation's risk profile and specific needs" and identifies three company-specific factors for prosecutors to evaluate:

Communications Channels. Under this factor, prosecutors should consider (1) the variability in the corporation's communications practices by jurisdiction and business function, (2) the mechanics the corporation has in place to manage and preserve information, (3) the preservation and deletion settings available to each employee, and (4) the rationale for the corporation's approach to determining which communication channel and setting is permitted.

Policy Environment. Under this factor, prosecutors should consider the corporation's relevant policies and procedures related to data preservation, privacy, and security, including the corporation's ability to monitor or access business-related communications.

Most significantly, if the corporation has a "bring your own device" (BYOD) program, this factor directs prosecutors to evaluate (1) the policy governing preservation of and access to corporate data and communications stored on personal devices, including data contained on messaging platforms; (2) the rationale for the policy; (3) the application and enforcement of the policy; and (4) any exceptions to the policy.

Risk Management Processes. Under this factor, prosecutors should consider the consequences for employees who refuse to allow the corporation access to corporate communications, including whether and how the corporation disciplines its employees. This factor also evaluates whether the use of personal devices or messaging applications (including ephemeral messaging applications) has impaired the corporation's compliance programs or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement agencies.

Ultimately, this factor asks whether the corporation's approach to permitting and managing communication channels is "reasonable in the context of the company's business needs and risk profile."

As part of the revisions, Polite also stressed the importance of cooperation by companies in the preservation and disclosure of digital communications, warning that "[d]uring the investigation, if a company has not produced communications from these third-party messaging applications, our prosecutors will not accept that at face value." Instead, companies must be prepared to explain their policies and procedures and to justify any limitations in their productions due to available technology or applicable privacy and local laws, among other factors. Ultimately, "[a] company's answers—or lack of answers—may very well affect the offer it receives to resolve criminal liability."

Recent Enforcement Actions Brought by Regulators for Failure To Preserve Ephemeral Messages

The revisions to the ECCP follow several noteworthy enforcement actions brought by the U.S. Securities and Exchange Commission (SEC) in recent years, further highlighting the importance of preserving ephemeral messages—including the real-world consequences for failure to do so. Notably, SEC rules provide that broker-dealers must preserve "[o]riginals of all communications received and copies of all communications sent . . . relating to its business," regardless of form, for a period of not less than three years, the first two years in an "easily accessible place."

Sixteen Wall Street Firms Fined $1.1 Billion for Failure To Preserve Text Messages. In September 2022, the SEC fined sixteen Wall Street firms more than $1.1 billion in total for "widespread and longstanding failures by the firms and their employees to maintain and preserve electronic communications." The SEC discovered that, between January 2018 and September 2021, the firms' employees regularly discussed business matters on their personal devices through various text messaging applications but failed to preserve the off-channel communications. The SEC alleged that the firms' failure to preserve the communications likely interfered with the SEC's investigation. As part of the settlement, the firms admitted that their conduct violated federal securities laws and agreed to implement improved compliance policies and procedures.

The Commodity Futures Trading Commission (CFTC) also separately settled with 11 of the firms, ordering them to pay more than $710 million for failure to "maintain, preserve, or produce records" pursuant to CFTC recordkeeping requirements and failure to "diligently supervise matters related to their businesses."

J.P. Morgan Securities LLC (JPMS) Fined $125 Million for Neglecting To Enforce Data Preservation Policy. In December 2021, the SEC fined JPMS $125 million for similar conduct. Specifically, the SEC discovered that from January 2018 through November 2020, JPMS employees at all levels regularly discussed business matters on personal devices using various messaging platforms, including WhatsApp and text messages. Despite JPMS's policies prohibiting their employees from utilizing personal messaging applications to discuss business-related matters, the SEC found that JPMS failed to properly supervise and enforce compliance with both their policies and federal securities laws. Further, the SEC found the failure to preserve the communications directly "impacted the SEC's ability to investigate potential violations of the federal securities laws."

Additionally, the CFTC ordered JPMS to pay $75 million for "widespread use of unauthorized communication methods" to conduct business-related matters and failure to adequately maintain internal controls regarding such communications.

JonesTrading Institutional Services, LLC (JonesTrading) Pays $100,000 Civil Penalty for Failure To Preserve Business-Related Text Messages on Personal Devices. In September 2020, the SEC settled charges against JonesTrading for failure to maintain and preserve text message communications on mobile devices regarding business matters. The SEC's order found that senior-level employees were among those who utilized personal devices to communicate about business matters. Unlike the prior two cases, JonesTrading did not admit or deny the SEC's findings but agreed to be censured, to pay a $100,000 civil penalty, and to cease and desist from violating federal securities laws.

Takeaways

Electronic communications have long played an important role in corporate investigations. The DOJ's new policy is a sign of the agency's desire to adapt to the times, making clear that a company's approach to preserving and accessing electronic communications—in whatever form they may take as technology evolves—will now be a critical part of any DOJ compliance evaluation.

This new DOJ guidance, combined with prior SEC enforcement actions on this topic, will likely also raise the expectations of other enforcement agencies, and similarly affect discovery in private party lawsuits. For companies that have not already crafted a careful acceptable use policy and adapted their document preservation policies to cover personal devices and all potential communications platforms, now is the time to act. For those who have such policies, it is advisable to audit compliance, identify gaps, and take action to ensure that those policies are being effectively and consistently enforced.

Authors

Explore more in

White Collar & Investigations Securities Litigation

Related insights

Update

Two Tools for Trump To Dismantle Biden-Era Rules: the Regulatory Freeze and the Congressional Review Act

Update

The FY 2025 National Defense Authorization Act: What’s New for Defense Contractors