Updates
November 28, 2022
New DOJ Guidance on Personal Devices and Third-Party Messaging Applications Applies to Any Company DOJ May Scrutinize

The U.S. Department of Justice (DOJ) recently released new guidance announcing several policy changes to further strengthen and clarify its approach to prosecuting corporate crime. The guidance, released through a memorandum by Deputy Attorney General Lisa Monaco (the Monaco Memo), instructs prosecutors about factors to consider when evaluating corporate cooperation and compliance programs in the context of potential criminal resolutions. Notably, the Monaco Memo advises that "prosecutors should consider whether the corporation has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms to ensure that business-related electronic data and communications are preserved." This guidance is applicable to all third-party text and social media messaging platforms, and it is especially significant given the recent proliferation of business use of ephemeral messaging applications that provide an option to have messages automatically disappear from a recipient's conversation history.

Companies would be wise to promptly review their business communications policies and procedures, in light of both possible DOJ oversight, as well as emerging privacy, security, and employment law scrutiny.

Who Is Covered?

Although many regulated entities such as broker-dealers and public companies already have record-keeping requirements under the securities laws and other applicable regulations, the Monaco Memo's pronouncement is applicable to *all* companies with any nexus to the United States. Indeed, any company—regardless of size, industry, or location—that may find itself one day before the DOJ seeking to show that it has a robust and effective compliance program would be wise to thoroughly review its policies regarding the use of personal devices and third-party messaging applications. Failure to adopt appropriate policies in this regard would violate now-clearly stated DOJ expectations, resulting in a loss of credit for an effective compliance program in the context of a future DOJ investigation into the company's conduct.

What Is Required?

In describing the DOJ's expectations, the Monaco Memo states: "As a general rule, all corporations with robust compliance programs should have effective policies governing the use of personal devices and third-party messaging platforms for corporate communications, should provide clear training to employees about such policies, and should enforce such policies when violations are identified."

The memo does not elaborate beyond those general guidelines. Instead, the Criminal Division will study best corporate practices regarding the use of personal devices and third-party messaging platforms and publish its findings in the next edition of its Evaluation of Corporate Compliance Programs.

How Should Firms Proceed?

While they wait for the DOJ to issue its findings, however, companies are not entirely without guidance in this area. Less than two weeks after the Monaco Memo was released, the U.S. Securities and Exchange Commission (SEC) and the U.S. Commodity Futures Trading Commission (CFTC) announced settlements with numerous financial institutions that had failed to preserve and supervise their employees' business communications on personal devices and third-party messaging platforms. As part of the settlements, each of the settling firms agreed to undertake certain remedial measures, including reviewing and improving their policies, training, technological solutions, surveillance, and discipline regarding business communications. In the absence of more specific requirements from the DOJ, those undertakings may serve as an emerging roadmap for what an effective personal devices and third-party messaging platforms compliance program should include.

Establish Clear Policies

Firms should ensure their written policies require all business communications to be preserved for a specified period of time, no matter the platform used. Companies should consider policies not only for employees, but also for directors and independent contractors (collectively referred to as "workforce members"). It may be advisable to have workforce members periodically acknowledge receipt and understanding of, and compliance with, these policies.

The policies should define what constitutes a "business communication" and clearly identify which devices and applications are permitted and which are prohibited. Permitted applications should be limited to those that the firm can use to collect and produce business communications in a reliable and timely fashion. In identifying permitted platforms, companies should solicit input from key departments such as information technology (IT) and security, human resources, and legal (especially with respect to enforcement of data subject rights and litigation holds).

The policies should make clear that if a workforce member stores any business information on their personal device or uses an unauthorized device or third-party messaging platform for business, the company will have the right to access the device and copy relevant data. If a workforce member deviates from policy, they should be subject to discipline, up to and including termination of employment. Companies also should evaluate realistically whether they have sufficient resources to monitor compliance with the policies.

Business communications policies often have profound employment law implications. For example, an employer may have wage-and-hour issues if hourly workers receive or respond to business communications while "off the clock." Similarly, workforce members may be entitled to on-call pay while they are waiting for instructions or interrupting protected sick or family leave. And even in a nonunion setting, employer surveillance of business communications may lead to potential violations of the National Labor Relations Act (NLRA). Companies should ensure that their business communications policy is consistent with any employee handbook and a multitude of other policies, including but not limited to: bring your own device (BYOD), acceptable use, social media, confidentiality, privacy, and record retention.

Comply With Existing Record-Keeping Obligations

As a baseline, companies should make sure they are complying with all industry or location-specific record-keeping obligations. For example, federal securities laws require public companies to make and keep accurate

"books, records and accounts." Certain employers may be subject to detailed rules requiring administrative, technical, and physical safeguards around data privacy and security and extended data retention periods, such as those applicable to healthcare companies under the Health Insurance Portability and Accountability Act (HIPAA) and financial institutions under the Gramm-Leach-Bliley Act (GLBA).

Beginning January 1, 2023, in sweeping legislation that is the first of its kind, the California Privacy Rights Act (CPRA) will require certain companies to extend data subject rights to applicants, employees, and independent contractors residing in California. That law, and its forthcoming regulations, will contain new obligations regarding data tracking, retention, and disclosure that will make the distinction between business records and personally identifiable information even more important. Similar legislation is expected in other jurisdictions in the near future, and the cost and burden on companies to comply with these requirements can be significant.

As new record-keeping requirements are adopted by state and federal regulators, companies should continuously monitor and update their business communications policies to ensure they meet evolving standards in this area.

Provide Adequate Training

Companies should provide clear, periodic training on the policies and provide resources where workforce members can turn with questions. Importantly, firms should ensure that senior management and supervisors understand the policies and are setting the right tone from the top. As the Monaco Memo states, the DOJ will be especially focused on "how senior leaders have, through their words and actions, encouraged or discouraged compliance."

Research Technological Solutions

Where companies know or reasonably should know that their workforce members use texting and ephemeral messaging applications for business, they should assess the relevant technology and offer workforce members options that allow critical business data to be collected and retained. In many countries, the use of ephemeral applications has become so ubiquitous that they have surpassed traditional text messaging and voice calls.

Companies should evaluate whether to provide workforce members firm-issued mobile phones pre-loaded with applications designed to retain or encrypt data, or to permit workforce members to BYOD as long as they install firm-mandated software that "sandboxes" and retains company data in an isolated environment. Businesses that adopt BYOD environments also should be mindful of state and local laws that require reimbursement of costs workforce members incur for business-related technology and service plans.

Monitor and Enforce Compliance

The Monaco Memo states that the DOJ will be looking at whether the company has "enforced" its policies when violations are identified. To do so, companies will need to find an appropriate, risk-based process for monitoring workforce members' compliance with the policies. Importantly, the policies should be enforced with appropriate discipline when violated, regardless of the workforce member's title. Inconsistent application of the policy could subject the employer to claims of employment discrimination, as well as generally undermining any claim that the company is committed to these policies and their effectiveness.

Each company has unique policies, procedures, risk tolerances, and corporate culture with respect to business communications. Given the multidisciplinary issues and high stakes involved in light of the DOJ's recent guidance, companies should work closely with experienced counsel to balance compliance risk with business necessity.

Authors

Explore more in

White Collar & Investigations Privacy & Security Investment Management Labor & Employment Fintech & Payments

Related insights

Update

FTC Announces New Children’s Privacy Requirements in Updated COPPA Rule

Update

Securities Enforcement Forum New York 2025: A New Era Looms