PAUL HASTINGS

Stay Current

March 2023

Follow @Paul_Hastings

DOJ's Approach to Ephemeral Messaging is Not Ephemeral: New Guidance on Messaging, Personal Devices

By Leo Tsao, Nisa R. Gosselink-Ulep, Brian Wilmot & Laurel Sutherland

On March 3, 2023, Assistant Attorney General Kenneth A. Polite announced[1] significant revisions to the Department of Justice ("DOJ") Criminal Division's Evaluation of Corporate Compliance Programs ("ECCP")[2] specifically focused on how compliance programs should account for risks from the use of personal devices and messaging applications. This new guidance builds upon earlier policy statements by the Criminal Division, first announced in 2017 as part of its Corporate Enforcement Policy, that have sought to encourage companies to manage these risks as part of their compliance programs and to ensure that evidence of potential misconduct is preserved.[3] Under the new ECCP, DOJ will now consider: (a) how policies relating to personal devices and messaging applications are "tailored to a company's risk profile," (b) how policies ensure that business-related data can be "preserved and accessed," (c) how the policies are communicated to employees, and (d) how companies monitor and enforce compliance by employees.

Compliance Risks Posed by Personal Devices and Messaging Applications

Business communications that once occurred almost exclusively on corporate e-mail systems and through company-owned computers and devices are now conducted on a wide range of communication platforms, including various messaging applications, and employee personal devices. This evolution in how employees conduct business communications creates challenges for preservation.

Companies rely upon messaging applications in their business, including everything from the more business-focused messaging platforms of Microsoft Teams and Slack to the ephemeral messaging applications like Whatsapp, Signal, WeChat, and Telegram, to name only a few. Ephemeral messaging applications are the most difficult platforms for companies to manage. These applications involve, as their name suggests, fleeting and short-lived messages that are typically accessed through mobile devices. They offer users the ability to send messages that automatically disappear from conversation histories, some by design and others at the user's option. There is a rapidly expanding and diverse ecosystem of such applications used around the world.

Business-focused messaging applications, when properly configured and implemented, often allow companies to properly monitor and preserve communications that occur through their platforms. This capability can be diminished when employees use these applications on personal devices or on devices without appropriate security and technical controls, such as device management software. In contrast,

ephemeral messaging applications emphasize secure communications and protection from monitoring, and may be used to frustrate attempts to preserve communications, notwithstanding any technical measures taken by a company to control communications on employee devices. These platforms thus pose significant compliance-related challenges to employers through their use of encryption and the automatic or periodic deletion of messages.

Why Are Personal Devices and Ephemeral Messaging Important to DOJ?

The issue of ephemeral messaging is important to DOJ for two main reasons. First, DOJ expects that an effective compliance program will have policies that allow it to collect and preserve business communications. Access to such communications is important for detecting misconduct and investigating potential misconduct. Second, DOJ often relies upon such communications not only as a contemporaneous record of what happened, but also to reveal the knowledge and intent of individuals. The loss of such business communications may impair DOJ's ability to conduct its own investigations.

The widespread use of messaging applications, combined with the increased use of personal devices for business, complicates companies' ability to control their use, monitor business activities within their organizations, and investigate and address misconduct. Business communications that previously occurred over email, and were centrally preserved by companies in accordance with a defined documented retention schedule, now exist only on an employee's personal device, if not automatically deleted. Companies have little or no control over these communications, and may have a limited basis to request access to them.

New Department of Justice Guidance

The ECCP provides guidance to federal prosecutors regarding how to evaluate companies' compliance programs. It also serves as a guide to companies themselves regarding what the Criminal Division expects companies to do when designing, implementing, and testing their compliance programs. The new guidance regarding ephemeral messaging and "bring your own device" ("BYOD") policies falls under one of the hallmarks of an effective compliance program: the investigation of misconduct.

Under this guidance, the Criminal Division will expect companies to treat messaging and personal device use as a standard part of their compliance program, including as part of their standard risk assessment process, compliance program development and enhancement cycle, and compliance monitoring and testing program. A policy addressing messaging and personal device use will not be enough, if that policy, and any other controls, are not effective in ensuring appropriate preservation of messaging application communications.

The Criminal Division acknowledges in the new ECCP that messaging applications "offer important platforms for companies to achieve growth and facilitate communication." It also offers three main categories of considerations for prosecutors assessing a company's handling of messaging platforms when evaluating a "corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law." Prosecutors will consider the following types of questions when doing so:

- **Communication Channels**: Which messaging applications do employees use, how do they use those applications, including on personal devices, where do they use these applications, and what limits does the company impose on the use of messaging applications and personal devices?

- **Policy Environment**: What are the "relevant code[s] of conduct, privacy, security, and employment laws or policies that govern" access to business-related communications and that impact the use, controls, and monitoring of messaging application and personal device use for the company?

- **Risk Management**: How does the company implement consequences for non-compliance with company policies regarding messaging and personal device use and determine whether its policies and controls are tailored to the company's risk profile and effective at preserving business communications necessary for it to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies?

These areas of focus are not surprising. They reflect similar expectations to those relevant to corporate compliance programs in general. Here, however, the Criminal Division is emphasizing that companies should take steps to:

- Understand the risks to their organization from ephemeral messaging and messaging tools more broadly, including what platforms are used, where they are used, and how they are used;

- Consider the full range of relevant policies and business processes that factor into a company's ability to holistically manage the risks of messaging applications and the use of personal devices; and

- Implement enforceable consequences and effective and tested control measures tailored to manage how messaging applications and personal devices are used in practice, account for the impact of messaging applications and personal device use on the company, and meet the risk profile of the company.

Key Takeaways and What Companies Can Do

There are no one-size-fits-all solutions for managing the risks presented by ephemeral messaging and personal devices. As the revised ECCP recognizes, it is not realistic for companies to simply block or ban the use of ephemeral messaging platforms. Rather, companies will be expected to balance the risks with the cost and feasibility of compliance measures and controls. How prosecutors assess compliance policies in practice with respect to ephemeral messaging and personal devices remains to be seen. In the meanwhile, companies should consider the following:

- Collecting information to understand how employees are using messaging platforms and personal devices in their organization, and conducting assessments to understand the risks posed by the use of those platforms and devices.

- Implementing clear and enforceable policies and controls that address ephemeral messaging and personal device use as applicable to the particular risks of the organization, and that facilitate company access to, and preservation of, business communications.

- Consider alternative messaging applications that permit preservation of communications while enabling business activities.

- Training employees regarding the policies addressing ephemeral messaging and BYOD, including expectations for use of messaging platforms and devices for business communications and requirements for retention of such communications.

- Enforcing those policies in good faith with appropriate consequences and discipline for non-compliance.
- Monitoring and testing policies and controls governing ephemeral messaging and personal devices to identify non-compliance and determine effectiveness, and if appropriate, taking necessary remedial steps.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Washington, D.C. lawyers:

Nisa R. Gosselink-Ulep
1.202.551.1746
nisagosselinkulep@paulhastings.com

Leo Tsao
1.202.551.1910
leotsao@paulhastings.com

Brian Wilmot
1.202.551.1981
brianwilmot@paulhastings.com

[1] Press Release, Assistant Attorney General Kenneth A. Polite Jr. Delivers Keynote at the ABA's 38th Annual National Institute on White Collar Crime (March 3, 2023), https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-keynote-aba-s-38th-annual-national.

[2] DOJ, Evaluation of Corporate Compliance Programs (March 2023), https://www.justice.gov/opa/speech/file/1571911/download.

[3] Paul Hastings Client Alert, Ephemeral Messaging at the Office: Avoiding Pitfalls and Establishing Best Practices (October 7, 2022), https://www.paulhastings.com/insights/client-alerts/ephemeral-messaging-at-the-office-avoiding-pitfalls-and-establishing-best.