LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
TUESDAY, OCTOBER 3, 2023

PERSPECTIVE

EXCEPTIONALLY APPPEALING

Don’t take it personal, but that device you’re using for work isn’t confidential

By Sheila A.G. Armbrust and Ankur Shingal

Shutterstock

Text message. iMessage. Signal. Telegram. WeChat. WhatsApp. Chances are, some of your employees, in some jurisdiction, are using at least one of these messaging applications to communicate about their work on personal devices used for business (BYOD devices). And the U.S. Department of Justice has indicated that, in the event of an internal or government investigation, it expects companies to collect and review work-related messages sent on their employees’ BYOD devices through these third-party applications.

Over the past 12 months, the DOJ has announced notable changes related to corporate policies regarding the use of personal devices for work. First, on Sept. 15, 2022, Deputy Attorney General Lisa Monaco issued a 15-page memo discussing revisions to the DOJ’s Corporate Enforcement Policy (the “Monaco Memo”). Among other announcements, the Monaco Memo states that the DOJ will more closely scrutinize corporate policies related to personal devices and third-party messaging applications. The Monaco Memo further defines a “robust compliance program” as one that collects work-related data from employees’ personal devices and third-party messaging applications. The Monaco Memo also identifies the “use of ephemeral and encrypted messaging applications” as areas of focus and issued a directive to the DOJ’s Criminal Division to “further study best corporate practices regarding use of personal devices and third-party messaging platforms and incorporate the product of that effort into the next edition of its Evaluation of Corporate Compliance Programs [ECCP.]”

Six months later, on March 3, 2023, and in keeping with DAG Monaco’s September directive, the DOJ updated the ECCP to include new guidance for prosecutors to evaluate “a corporation’s policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications.” The DOJ announced three factors that prosecutors should consider in evaluating a corporate compliance program:

(1) The corporation’s knowledge about the electronic communications channels its employees use across business functions and jurisdictions and its management of settings related to preserving or deleting communications;

(2) The corporation’s policies regarding electronic devices, including access to and preservation of data from BYOD devices, including devices that are being replaced; and

(3) The corporation's management of risks associated with use of BYOD devices or third-party messaging applications, including discipline for employees who fail to comply with company policies and assessment of whether ephemeral messaging applications impair the organization's internal compliance functions.

That same day, while speaking at the American Bar Association's annual National Institute on White Collar Crime, then-Assistant Attorney General Kenneth A. Polite, Jr. described these changes to the ECCP as "significant," including because of those changes pertaining to how corporations approach "use of personal devices as well as various communications platforms and messaging applications, including those offering ephemeral messaging." Then-AAG Polite explained that a company's failure to preserve and produce such messaging data could affect a plea offer that it receives.

The DOJ's increased focus on the use of personal devices follows the business reality that BYOD policies and messaging applications are a new normal. This is in no small part due to the explosion of remote and hybrid work environments since the onset of the COVID-19 pandemic. Indeed, a 2022 study found that "83% of companies have a BYOD policy of some kind," and that many employees may be using text messaging or ephemeral messaging to communicate with their co-workers about work.

Employees' use of personal devices and third-party messaging applications can also cause challenges related to how different organizations within a company may communicate with each other or with others outside of the company. For instance, unless there is adequate company oversight and appropriate policies are in place, it is possible that a communication regarding an urgent compliance question from a sales representative might be sent to the compliance team via a third-party application, rather than through business email. The third-party application is outside the company's control and so the company may not be able to access that communication or use it to investigate potential wrongdoing in internal or government investigations.

Faced with the DOJ's increased emphasis on preserving and reviewing content from BYOD devices in investigations, the following are three practical considerations for companies preparing to create a robust compliance program in advance of a government investigation:

1. Educate employees about mixing work and personal communications. Employees should understand that if they use third-party applications for work on either a personal or work-provided device, all of the data from that application may be collected and reviewed by the company or the government. The prospect of such a review may dissuade employees from using third-party applications for work purposes, or encourage them to limit the numbers of applications that they use, while also ensuring that they understand the potential scope of any investigation. Early education also will allow for enforcement of policies that require collection of such third-party application data from employees in the event of an investigation.

2. Evaluate BYOD policies and accepted applications. Though the overwhelming majority of companies have some version of a BYOD policy, an employee's use of a personal device increases the possibility that the employee may download and use applications to send messages that the company does not have access to. Introducing a policy that provides mobile devices to employees, along with a requirement that substantive work discussions occur only on that work device, reduces the risk of lost data. Companies that continue with a BYOD policy could also consider providing a list of authorized applications that the company has access to, which would increase the likelihood that employees would use only those applications for work. Companies can also evaluate providing a business-managed instant messaging option like Teams, WebEx, or Slack, each of which offers companies greater control over and access to employee messaging. A further step, in situations where employers provide a work device, is to require administrative privileges to download any unauthorized applications. Finally, companies that provide BYOD stipends or mobile data reimbursements could also condition these payments on employees' agreements to make their devices accessible to the company.

3. Poll employees now - in advance of an investigation - about what applications they are using. Companies should proactively conduct a risk assessment to understand what applications employees are using, where in the organization they are using these applications, in what jurisdictions, and what risks those applications pose. That will ensure that companies are able to better design compliance programs and begin any required risk assessment before an internal or governmental investigation arises.

Sheila A.G. Armbrust *is a partner at Sidley Austin LLP in San Francisco. She can be reached at sarmbrust@sidley.com.* **Ankur Shingal** *is a senior managing associate with Sidley Austin LLP in Chicago. He can be reached at ashingal@sidley.com.*