LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
FRIDAY, DECEMBER 11, 2020

PERSPECTIVE

Guidance for developing third-party messaging app policies

By Jack P. DiCanio
and Emily A. Reitmeier

In 2019, the U.S. Department of Justice announced an important change to its Foreign Corrupt Practices Act Corporate Enforcement Policy concerning one of the conditions that companies must meet to receive "full credit" for "timely and appropriate remediation" in the resolution of an FCPA enforcement action. The DOJ declined to require an outright ban on the use of third-party instant messaging applications. Rather, companies must demonstrate their "ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations," and were given the latitude on the chosen means to do so — i.e., by implementing "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms."

Third-party messaging apps that use ephemeral features (i.e., where messages automatically disappear from the recipient's screen) can be useful in conducting business, especially in certain countries where there are concerns about government interception of non-encrypted communications. Moreover, with increasing use of electronic communication (rather than phone calls, letters, or in-person communications), especially in light of the COVID-19 pandemic, a company faces very real costs and burdens associated with storing and processing large amounts of electronic data. Use of instant messaging apps can help alleviate some of that burden for unimportant or nonmaterial communications that do not need to be maintained.

The DOJ has not issued any additional formal guidance to assist companies in deciding what controls are appropriate when using these apps and how such controls should be implemented. In the event of an FCPA investigation, companies may be second-guessed by the DOJ about the use of these apps, especially in hindsight, and therefore should carefully evaluate the adequacy of their internal policies and practices with that consideration in mind.

First, companies should be thoughtful in how they develop a communications policy which addresses the use of third-party messaging apps. What is "appropriate" will vary based on many factors such as the type of business being conducted and the country where the business is occurring. For example, in certain countries, such as China, India and Russia, third-party encrypted messaging apps are used extensively for legitimate business communications — sometimes to the exclusion of corporate email. This is due, in part, to legitimate concerns about government interception of non-encrypted communications. As a result, companies may not be able to adequately communicate with their customers without using these apps, and use of these apps in such countries can be deemed necessary.

The DOJ has not issued any additional formal guidance to assist companies in deciding what controls are appropriate when using these apps and how such controls should be implemented.

The key to developing a third-party app communications policy, like any compliance policy, is to take a thoughtful and risk-based approach. Compliance officers should talk to management and employees to understand customs and practices and the need for such communications. Understanding how and why these apps are used will assist the company in making a risk-based judgment to create its policy.

Second, companies should develop a policy to ensure proper record keeping of communications occurring in these apps which constitute the "books and records" of the company. Under the FCPA, a company must take "reasonable" steps to maintain records which accurately and fairly reflect the transactions and dispositions of the assets of the business, but neither the FCPA nor the regulators provide specific guidance on what this entails. Again, a company should take a thoughtful, risk-based approach, especially since any policy may be second-guessed by the DOJ, especially in hindsight, during an investigation. For example, a company policy could delineate what important aspects of a deal

(e.g., first contact, pricing, delivery terms) must be documented in a written memorandum or in a confirmatory email, regardless of whether the communication occurred via third-party app or verbally. Additionally, for third-party messaging apps that allow backup and migration of messages, a company policy could require an employee to migrate and export the individual's work-related messaging history on a periodic basis or to schedule periodic backups in the app itself.

Third, companies should monitor compliance with these policies. This can help ensure that the use of the apps would not be seen by the government as evasive behavior and that there is no implication that these apps are used as a way to hide communications. The company should consider some method to test whether individuals are complying with the policy, possibly through its internal audit function. A company should also provide training, possibly in connection with annual code of conduct training, regarding the proper usage of third-party messaging for business-related communications.

Finally, a company should also consider whether it has a bring-your-own device policy, how that policy interacts with local data privacy laws, and how those policies could limit the company's ability to collect and preserve data from these apps. The company should revisit its bring-your-own device policy and review, for those jurisdictions in which third-party apps are permitted to be used, how and when the company can image a personal device. In some jurisdictions, the company may not be able to review or image the device if the employee does not consent. The company may want to consider providing company-issued devices in these jurisdictions for customer-facing employees (e.g., the sales team). Companies have a stronger case in foreign jurisdictions to image data from the device if the device is issued by the company and the employee is instructed not to use the device for personal use. This is important as the DOJ can view negatively the inability to collect data from a personal device of a key witness or target during an investigation because the witness's refusal to consent to collection.

Additionally, if a company has a bring-your-own device policy, the company may want to consider requiring employees to establish separate user accounts in the apps for business and personal uses to mitigate potential privacy issues should the company need to collect data from the app.

The bottom line is that while the use of third-party messaging apps for conducting business can be useful and preferred. a company should be mindful of the DOJ's view of these apps when developing internal policies for their use, even when dealing with the most well-intentioned employees and companies. Companies should proactively and periodically revisit these policies to ensure they are justified, defensible, and to help bring them in line with the DOJ's policy and expectations. Developing a strong, risk-based policy and taking steps periodically to ensure compliance with the policy will best position the company to argue that it should receive full cooperation credit in any FCPA investigation. ■

Jack P. DiCanio *is a litigation partner at Skadden, Arps, Slate, Meagher & Flom LLP. You can reach him at jack.dicanio@skadden.com.*

Emily A. Reitmeier *is litigation counsel at Skadden, Arps, Slate, Meagher & Flom LLP. You can reach her at emily.reitmeier@skadden.com.*