Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Clarifications Needed After DOJ's New FCPA Policy

By **Derek Hahn, Dalal Hasan, Tom Hanusik and Stephen Byers** (March 22, 2019, 4:29 PM EDT)


Derek Hahn


Dalal Hasan


Tom Hanusik


Stephen Byers

The U.S. Department of Justice released revisions to the Foreign Corrupt Practices Act corporate enforcement policy on March 8, 2019.[1] While intended to clarify the DOJ's position on a number of hot-button issues, including its controversial stance on certain instant-messaging software, a closer look reveals that these changes fall short of answering several key questions faced by companies seeking cooperation credit in FCPA matters.

The FCPA Corporate Enforcement Policy

Originally formalized in November 2017 following a pilot program, the policy provides significant incentives to companies that voluntarily self-disclose FCPA violations, cooperate with the government, and appropriately remediate. Companies that self-disclose can expect a presumption of a declination of criminal charges, or, where enforcement is warranted, a 50 percent fine reduction off the low end of the applicable U.S. sentencing guidelines range. If a company does not self-disclose, but still fully cooperates and remediates, it can earn up to a 25 percent fine reduction.

Those incentives remain intact in the revisions. The changes instead attempt to clarify DOJ's position on a range of issues that have arisen since the policy was implemented, including: deconfliction requests, the "relevant facts" a company must disclose, waiver of the attorney-client privilege, the applicability of the policy to violations unearthed in the context of mergers and acquisitions, and the retention of records within certain instant-messaging applications.

Instant-Messaging Software

Under the old policy, companies seeking to receive full credit for "timely and appropriate remediation" were expected to "prohibit the improper destruction or deletion of business records, including prohibiting employees from using software that generates but does not appropriately retain business records or communications."[2]

This language could easily be read to prohibit the use of ephemeral messaging applications such as SnapChat, which are designed to delete communications. Less clear was whether the prohibition extended to any type of personal, third party

instant-messaging application that did not retain communication records within a company's information technology systems, as opposed to on personal devices — including widely used applications such as WhatsApp or even ordinary text messaging.

The DOJ's revised policy replaces the prohibition language with a requirement to implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."[3] The specific edits are shown here:

- Appropriate retention of business records, and prohibiting the improper destruction or deletion of business records, including ~~prohibiting employees from using software that generates but does not~~implementing appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations; and

In sum, the DOJ changed the language from prohibiting software that does not "appropriately retain" records to requiring "appropriate guidance and controls." This appears to provide companies more flexibility in this area rather than impose flat-out prohibitions. Unfortunately, the practical significance for companies seeking cooperation credit under the policy are likely unchanged for two reasons.

First, the DOJ has now clarified that it is concerned with both "personal communications" and "ephemeral messaging" platforms. This confirms that popular personal communication applications like WhatsApp are encompassed, even if they are not designed to be ephemeral.

Second, the requirement to implement "appropriate guidance and controls" on the use of personal communications applications may effectively operate as a prohibition, notwithstanding the DOJ's removal of that term. The DOJ clearly wants access to these records during its investigations. But retaining business records within personal messaging applications could require intrusive, expensive, and operationally complex protocols that raise a host of issues:

- Practical challenges: Employees often communicate using multiple devices and applications that may be technically challenging to synchronize with company servers or otherwise retain. And enterprise versions of many of these applications are either not available or prohibitively expensive, and even if adopted, employees may not use them exclusively.

- Ethical implications: Attempting to retain business records in personal communication applications may intrude into the private lives of employees to the extent personal information is accessed or captured (even unintentionally) as part of the process.

- Legal restrictions: Existing and emerging data privacy and labor laws — applicable to the employees and the third parties with whom they communicate — may prohibit companies from accessing or collecting information from personal devices or personal accounts, even if it is business related and perhaps even if consent is obtained.

Companies that are unable to overcome these issues may opt to prohibit these applications. A prohibition, however, comes with its own challenges. Enforcement would be difficult as it may require

monitoring the use of personal devices or personal applications — again likely implicating data privacy issues. A prohibition could also impact operations negatively where the use of such applications is prevalent in the local business community.

Companies seeking to comply with the policy will have to grapple with crafting "appropriate guidance and controls" until the DOJ clarifies its expectations through additional guidance, commentary or enforcement actions. It is important to remember, however, that these requirements pertain to the DOJ's FCPA enforcement policy; the DOJ is not creating a new legal obligation to retain these records. Of course, companies likely already have independent business reasons for appropriately controlling business records created with messaging applications. The potential for receiving cooperation credit in a future FCPA enforcement action is one more factor to consider when addressing this complex issue.

Deconfliction

The original FCPA policy required companies seeking cooperation credit to "deconflict," or defer, witness interviews and other internal investigative steps upon request and in deference to the government's investigation. Such requests were to be made for a limited period of time and narrowly tailored to a legitimate investigative purpose.

Deconfliction requests and other government actions can implicate employees' due process rights where they exert so much control over a company's internal investigation that the company effectively becomes an agent/extension of the government.

Responding to these concerns, the DOJ amended its policy to state that it "will not take any steps to affirmatively direct a company's internal investigation efforts" and emphasized that it will only request deconfliction "where appropriate." However, appropriateness is in the eye of the beholder — often a court — and whether the DOJ changes its approach to deconfliction or its broader role in internal investigations remains to be seen. Moreover, regardless of whether "affirmative" action or simply inaction is requested, deconfliction requests can often conflict with a company's need to prepare audited financials, fulfill regulatory obligations and/or its fiduciary obligations to shareholders.

Disclosure of "All Relevant Facts"

The DOJ's position on the scope of "relevant facts" a company must disclose to obtain cooperation credit has evolved in recent years, and the FCPA policy now appears to be catching up — at least in part.

The Justice Manual's section on Principles of Federal Prosecution of Business Organizations sets forth the threshold requirements for cooperation credit applicable in DOJ civil and criminal corporate investigations.[4] As articulated in the September 2015 Yates memorandum, the DOJ previously required complete disclosure of all relevant facts for "every person involved" in order to receive any cooperation credit.

The original FCPA policy, which is contained in a separate section of the Justice Manual,[5] also addressed expectations for disclosure of relevant facts regarding individuals in two sections: voluntary disclosure and cooperation credit. Like the Yates memo, the FCPA policy's original voluntary disclosure provisions required companies to provide all relevant facts about all individuals "involved in" the violation of law. Similarly, for cooperation credit, the FCPA policy required disclosure of all relevant facts related to those with "involvement in" the criminal activity.

In November 2018, the DOJ amended the Justice Manual to clarify that companies can obtain cooperation credit when they identify those who were "substantially involved in or responsible for wrongdoing" — rather than all individuals who were simply "involved." According to Deputy Attorney General Rod Rosenstein, this change reflected the DOJ's recognition that "it is not practical to require the company to identify every employee who played any role in the conduct."[6] Instead, the DOJ would "focus on the individuals who play significant roles in setting a company on a course of criminal conduct."

The FCPA policy, however, continued to reflect the heightened standard, i.e., relevant facts regarding all individuals involved in the violation of law.

The DOJ has now changed the language in the voluntary self-disclosure section of the FCPA policy to match the less stringent requirements for general corporate cooperation credit. However, the DOJ left the heightened standard in the cooperation credit section of the FCPA policy untouched and this inconsistency renders the new language meaningless.

In summary, to get credit under the general cooperation provisions for all corporate cases and/or the revised voluntary self-disclosure provisions of the FCPA policy, companies must still "fully cooperate", but in theory only need to identify the facts about all individuals "substantially involved in or responsible for" the misconduct or violation of law.[7] However, to achieve credit for "full cooperation" under the FCPA policy, companies still have to disclose "all facts related to involvement in the criminal activity by the company's officers, employees, or agents" or those of third parties.[8]

Thus, the seemingly lower standard in the FCPA's voluntary disclosure section is irrelevant because "full cooperation" is still required under that provision and "full cooperation" is still defined in the same policy to require all facts about everyone's involvement in criminal activity, not just those substantially involved in or responsible for such activity.

Expect future clarifications from the DOJ.

Waiver of Attorney-Client Privilege

Companies seeking to meet the DOJ's broad requirement for disclosure of facts risk waiving privilege to deliver the information. This risk is compounded when there is related existing or threatened civil litigation. While the original FCPA policy contained language stating that cooperation credit was "not predicated upon waiver of the attorney-client privilege or work product protection," it did not address privilege in the voluntary self-disclosure context.

The new policy attempts to clarify that eligibility for "cooperation or voluntary self-disclosure credit is not in any way predicated" on waiver. While this language further entrenches the DOJ's official position that waivers are not required, it does not resolve the inherent tension between making the requisite factual disclosures and preserving the attorney-client privilege.

Violations Discovered During Mergers and Acquisitions

In a July 25, 2018, speech, Deputy Assistant Attorney General Matthew S. Miner announced that the DOJ would apply the presumption in favor of declination to successor companies in the mergers and acquisition context where they self-disclose, cooperate, and timely implement an effective compliance program at the merged or acquired entity.[9] This unwritten policy was formally inserted into the FCPA policy as part of the recent revisions.

Key Takeaways

DOJ expectations regarding the "appropriate guidance and controls" companies should adopt to retain business records on ephemeral and personal communication systems remain unclear. Until the DOJ offers more clarity, companies should continue to carefully craft policies that strike a defensible balance between employees' need to use such systems, the technical limitations on data retention inherent in them, the data privacy implications and the DOJ's expectations concerning record retention. Companies that choose to prohibit such systems should design appropriate training, monitoring and enforcement protocols, and consider enterprise equivalents to offer as an alternative.

Overall, the recent revisions to DOJ's FCPA enforcement policy reflect a continued trend toward encouraging companies to self-report and cooperate and away from requiring privilege waivers. However, no amount of policy revisions will eliminate the multifaceted risks of self-disclosure and cooperation in FCPA and other white collar cases. Staying attuned to regulator expectations — both formal and informal — is critical to successfully navigating those risks.

Derek Hahn is a partner, Dalal Hasan is a counsel, and Tom Hanusik and Stephen Byers are partners at Crowell & Moring LLP.

Matt Gander, an associate at the firm, contributed to this article.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Justice Manual § 9-47.120 (2019), https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.

[2] Justice Manual Section 9-47.120 (2018).

[3] Justice Manual § 9-47.120(3)(c) (2019), https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977.

[4] Justice Manual § 9-28.700 (2018), https://www.justice.gov/jm/jm-9-28000-principles-federal-prosecution-business-organizations#9-28.700.

[5] Justice Manual Section 9-47.120 (2018).

[6] Rod Rosenstein, Deputy Att'y Gen., Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act (Nov. 29, 2018), https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-institute-0.

[7] Justice Manual §§ 9-28.700 (2018) and 9-47.120(3)(a) (2019).

[8] Justice Manual § 9-47.120(3)(b) (2019) (emphasis added).

[9] Matthew Miner, Deputy Assistant Att'y Gen., Deputy Assistant Attorney General Matthew S. Miner Remarks at the American Conference Institute 9th Global Forum on Anti-Corruption Compliance in High Risk Markets (July 25, 2018), https://www.justice.gov/opa/pr/deputy-assistant-attorney-general-matthew-s-miner-remarks-american-conference-institute-9th.