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

Retaining Ephemeral Messages To Prepare For DOJ Scrutiny

By **Mark Rosman, Jeff Bank and Byron Tuyay** (July 29, 2019, 2:10 PM EDT)

Mark Rosman

Jeff Bank

Byron Tuyay

The Antitrust Division of the U.S. Department of Justice has long relied on documents to prove the existence of anticompetitive agreements in cartel cases. Indeed, it is not uncommon for cartel prosecutions to turn on the discovery of so-called "smoking gun" documents to confirm unlawful competitor agreements.

Technology over the last 15 years, however, has drastically changed where, when and how people communicate for work. Modern business communications take place across numerous devices and media, including email, messaging applications and a wide variety of productivity applications such as Slack, Skype for Business, Google Hangouts and Cisco Jabber.

Users tend to prefer the instantaneous nature of communicating, and they derive a sense of security and privacy from using messaging platforms that feature encrypted messages that disappear after a certain amount of time (i.e., ephemeral messaging). Employees can also embed documents, links or pictures in such messages. Such applications, though, can pose a significant hurdle to DOJ investigations and internal investigations alike as potential key evidence can literally disappear at users' fingertips. Other DOJ sections have begun to address such issues in the context of Foreign Corrupt Practices Act corporate enforcement, and the Antitrust Division may not be far behind.

In response to this developing challenge, recent Antitrust Division cartel investigations have focused on searching evidence from ephemeral messaging platforms. For example, indictments filed in the DOJ's investigation into the foreign currency exchange spot market featured prominently the defendants' "near-daily conversations in a private electronic chat room."[1]

Similarly, the DOJ's investigation into the online customized promotional products industry netted key evidence of a price-fixing conspiracy from social media platforms and encrypted messaging applications including Facebook, Skype, and WhatsApp [2] In fact, the Antitrust Division's internal training material for law enforcement personnel now explicitly advises that communications evidencing cartel conduct can be found via "Facebook message, WhatsApp, and encrypted messaging apps like Confide."[3]

Moreover, one judge's recent comments at a sentencing hearing regarding the use of "burner" phones suggests that some judges may view the mere use of ephemeral messaging apps — because of their temporary nature — as a factor demonstrating an individual's attempt to purposefully conceal unlawful communications.[4]

The widespread use of messaging apps in the workplace (domestic and foreign, large and small) signals an inevitable shift away from traditional documentary evidence (e.g., memoranda, meeting minutes and even emails) in cartel investigations. As explained below, this shift raises significant practical questions about the Antitrust Division's investigatory methods as well as whether companies should be required to take steps to preserve communications sent via ephemeral applications in order to be eligible for certain leniency or cooperation benefits. What's more, technological limitations and privacy issues may blunt the impact of any DOJ policy changes as companies continue to grapple with challenges to collecting and producing employee data.

FCPA Corporate Enforcement Policy Updates

Recent amendments to the DOJ's FCPA corporate leniency policy suggest that the DOJ recognizes the importance of messaging applications to workplace productivity but also confirm the value of preserving these potentially rich sources of evidence for corporate leniency applicants and, more broadly, to assist with law enforcement.

On March 8, 2019, the DOJ announced changes to its FCPA corporate enforcement policy, under which the DOJ would decline to bring charges only if a company adopted certain compliance and remediation practices related to ephemeral evidence. We expect that the Antitrust Division may at some point mirror some of these new policy requirements.

Before March 8, 2019, the DOJ required companies seeking FCPA leniency credit for remediation to internally prohibit employees from using messaging applications that did not appropriately retain business records or communications.

Now, just two years after the policy was formalized, the DOJ has reversed course and instead will require companies seeking FCPA leniency to implement "appropriate guidance and controls" on the use of disappearing messaging services such as WhatsApp, WeChat, Snapchat or other ephemeral messaging applications that could "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."[5]

This change relaxes the policy requirement, which had been criticized by the business community, including the U.S. Chamber of Commerce, for being too rigid. Observers have noted, however, that to date no public DOJ declinations issued under the FCPA corporate enforcement policy has cited a company's prohibition on ephemeral messaging software as a basis for conferring full credit for remediation.[6]

Nonetheless, the DOJ's policy change with respect to disappearing or ephemeral messaging applications now provides businesses with some flexibility to use their preferred workplace messaging applications, so long as the company implements appropriate safeguards. In theory, this means that companies that rely heavily on messaging applications for regular business communications can continue using such applications (and be eligible for leniency) if they confirm that the applications retain business

communications consistent with existing corporate retention policies and, if necessary, preserve records and communications pursuant to a litigation hold.

As a practical matter, however, it is unclear how companies will preserve business communications on ephemeral messaging apps that do not allow users to set data backup preferences. Certain messaging apps do not back up data once it is deleted. Absent such features, a company may opt to reevaluate its preferred messaging application rather than face the technological hurdles of using a messaging platform that, by design, is incompatible with traditional corporate retention policies.

Potential Impact on Antitrust Preservation Policy and Practical Considerations

The Antitrust Division's current corporate leniency policy does not explicitly address ephemeral messaging applications nor does it require leniency applicants to ban their use internally. Recent guidance issued by the Antitrust Division, however, confirms that a company can benefit at the charging phase of a criminal investigation if its compliance program addresses the antitrust risk posed by ephemeral messaging apps.

On July 11, 2019, the Antitrust Division published a guidance document intended to assist prosecutors in their evaluation of corporate antitrust compliance programs in criminal antitrust investigations. The guidance outlines several factors prosecutors must consider at the sentencing and charging phases of an investigation.

Among other factors, prosecutors will now consider whether the compliance program is appropriately tailored to account for antitrust risk and the company's efforts to implement policies that address "technical changes in the way the company conducts business" and "new methods" of electronic communication.[7] Thus, a compliance program that adequately accounts for the risks posed by ephemeral messaging applications may impact whether and to what extent the Antitrust Division will bring criminal charges against companies under investigation .

The Antitrust Division's recognition of compliance programs that address new communication technologies suggests that the division's longstanding corporate leniency policy for self-reporting companies seeking leniency and cooperation credit in plea negotiations may eventually track the FCPA corporate enforcement policy regarding messaging applications.

As noted previously, the Antitrust Division's cartel prosecutions have increasingly relied on evidence drawn from such messaging platforms. Moreover, to the extent that cartel investigations reach businesses in foreign jurisdictions, a policy that addresses the preservation of messaging application data may have a significant impact on cartel investigations, for example, in Asia where the use of personal messaging apps such as Line, Wechat, Telegram, Viber and Kakaotalk is deeply engrained in the local business culture.

If the Antitrust Division eventually adopts policies in line with the DOJ's current FCPA corporate leniency requirements, future leniency applicants or companies engaged in plea negotiations seeking cooperation credit will not be required to fully ban such messaging applications among employees. Instead, future companies seeking leniency or cooperation credit in cartel investigations might continue using these messaging applications in the ordinary course of business so long as they take steps to offer guidance and implement controls on personal communications and ephemeral messaging platforms such that business records and communications are appropriately retained or remain otherwise compliant with the company's legal obligations.

Importantly, the requirement to maintain these records may be especially important for "Type B" leniency applications, which are filed after the DOJ initiates an investigation, because in such cases the DOJ exercises discretion based, in part, on whether it has a provable case. Whether or not critical communication-based evidence exists and can be produced and reviewed will likely be a key determinative factor for the DOJ.

Yet, even if the Antitrust Division does not adopt formal policy changes, the widespread use of ephemeral messaging applications for business-related communications raises significant questions about future investigations. For instance, when companies or employees that are located in foreign jurisdictions are subject to an Antitrust Division investigation, can the agency effectively subpoena foreign providers such as Kakaotalk, Wechat and LINE Corp. that host the messaging data on servers abroad?

Relatedly, to what extent can (or will) the DOJ subpoena employee messages from their personal accounts where the local data privacy laws afford greater protections? Requiring companies that self-report to ensure the preservation of communications may help the Antitrust Division avoid these questions, or at least reduce their importance.

However, because the DOJ has not yet given guidance on what constitutes an appropriate compliance program relating to ephemeral messaging applications, we expect additional questions to be raised in the near future as to what steps a company must take to meet self-reporting requirements.

Implementing Appropriate Guidance and Controls

For companies and their in-house counsel, there are at least two key benefits of ensuring that document retention and preservation policies appropriately account for ephemeral messaging applications. First, a company that preserves access to its employees' business-related ephemeral messaging data will benefit from having more complete information when conducting an internal investigation (whether or not in response to an existing government investigation).

With greater insight into the potential evidence that such messaging data can hold, a company can make informed decisions about defensive or cooperative strategies in government investigations including the critical decision of whether the company should apply for leniency or engage with the DOJ at all. Second, as noted above, companies that implement appropriate safeguards with regard to employees' use of ephemeral messaging are well-positioned to receive remedial credit under the DOJ's current FCPA corporate enforcement policy (and potentially under Antitrust Division policy).

There are a number of steps that a company can take to implement appropriate safeguards surrounding the use of ephemeral messaging applications in the workplace.

Understand Employee Usage

As an initial step companies should take inventory of what, if any, ephemeral messaging applications its employees use or may use for business communications. Note that messaging applications tend to be specific to certain geographies, industries and/or positions. For instance, applications commonly used for business in Western Europe may vary from those used in Asia; those used in the banking industry may differ from those used in the technology industry and those used by marketing executives may differ from those used by sales executives.

Companies should identify which individuals or groups within the organization most frequently use such messaging applications for business and understand how the employees use them. For example, sales employees may ordinarily discuss pricing via email, but while traveling for customer visits they may send photos or screen shots of bid sheets as attachments to chats via a messaging application. Ultimately, understanding employee usage will allow companies to better conduct risk assessments and develop its policies.

Develop Adequate Internal Policies

Companies should develop internal policies that address the use of ephemeral messaging applications or supplement existing policies regarding the use of messaging platforms for business communications with third parties as needed. At a minimum, a company should address the use of ephemeral messaging applications in its document retention policy. If a company is unable to capture data from a particular messaging service, the company might consider implementing a formal policy requiring individuals using that messaging service to back up their own communications.

Regular monitoring may be necessary to ensure compliance. Device-management software such as AirWatch allows a company to regulate the apps used on work-issued devices. Companies can further limit the scope of certain employees' instant messages by approving the use of messaging apps that can restrict messages to external parties. Furthermore, requiring employees to establish separate user accounts for business and personal uses can mitigate risks of potential privacy issues if the necessity arises to preserve business communications from such applications.

Understand Local Privacy Regulations

Companies must carefully examine the privacy laws of any relevant jurisdictions to ensure that collection or disclosure of data is done in compliance with all governing regulations. In some jurisdictions, it may be prudent to require employees likely to be communicating on topics of interest (e.g., sales, pricing, bidding trade associations) to use company-issued devices instead of personal devices. This could mitigate the risk and challenges faced in attempting to collect and produce information from an employees' personal device.

Training

Issuing updated guidelines and holding regular meetings on the appropriate use of ephemeral messaging applications for business communications can reinforce best practices and avoid potential preservation issues.

Data Backup and Recovery Options

Companies should develop processes for backing up data on ephemeral messaging applications, if technologically feasible. This may require employee-users to enable features on the messaging applications that allow them to backup chat histories. Absent such features, a company may consult with information technology professionals to develop solutions for preserving business communications in line with current retention policies or future preservation obligations.

Regular Reassessment

Companies should periodically reassess messaging platform use in the work environment to ensure that internal policies and practices keep pace with new communication technology. Monitoring trends in employee messaging platform usage is particularly useful since the adoption rate of new messaging technologies varies by individual employees.

Conclusion

Companies that wish to use the latest messaging application technologies in their daily operations, or that know their employees are using such technologies, should be mindful of the DOJ's policy and considerations when selecting appropriate business communications platforms. Particularly given the increased focus on ephemeral messaging applications as a source for key evidence in government investigations, understanding the widespread use of these messaging applications in today's workplace is the first step a company can take toward adopting appropriate controls and policies.

Companies that commit to proactive compliance policies and set forth best practices, preservation and data backup options for ephemeral messaging applications are better positioned to respond nimbly to government investigations. Implementing such policies can cut costs, minimize disruption in the workplace and earn the company full remediation credit under the FCPA corporate enforcement policy or under the Antitrust Division's policy.

Mark Rosman is a partner at Wilson Sonsini Goodrich & Rosati PC. He previously served as assistant chief of the national criminal enforcement section in the U.S. Department of Justice's Antitrust Division.

Jeff Bank is a partner at the firm and previously practiced in the Federal Trade Commission's health care division.

Byron Tuyay is an associate at the firm.

[1] See "Three Former Traders for Major Banks Indicted in Foreign Currency Exchange Antitrust Conspiracy" https://www.justice.gov/opa/pr/three-former-traders-major-banks-indicted-foreign-currency-exchange-antitrust-conspiracy

[2] See "Justice Department Announces Multiple Charges for Price-Fixing Conspiracies in Customized Promotional Products Industry" https://www.justice.gov/opa/pr/justice-department-announces-multiple-charges-price-fixing-conspiracies-customized

[3] An Antitrust Primer for Federal Law Enforcement Personnel, U.S. Dep't of Justice Antitrust Division, September 2018, at 5 https://www.justice.gov/atr/page/file/1091651/download

[4] See "Ex-UBS Worker, Day Trader Get 3 Years For Insider Dealing" https://www.law360.com/articles/1173447/ex-ubs-worker-day-trader-get-3-years-for-insider-dealing.

[5] See Justice Manual, 9-47.120(3)(c) – FCPA Corporate Enforcement Policy, https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.

[6] "DOJ Revises Policy on Instant Messaging Apps in Foreign Corrupt Practices Act Enforcement," Bloomberg Law, April 18, 2019 https://news.bloomberglaw.com/us-law-week/insight-doj-revises-policy-on-instant-messaging-apps-in-foreign-corrupt-practices-act-enforcement

[7] "Evaluation of Corporate Compliance Programs in Criminal Antitrust Investigations" U.S. Dep't of Justice, Antitrust Div., July 2019, https://www.justice.gov/atr/page/file/1182001/download