Effective E-Discovery Of Chat Apps In Gov't Investigations

By **Jason Weinstein and Katie Dubyak** (February 19, 2021)

Jason Weinstein

Katie Dubyak

In the not-too-distant past, electronic discovery in a government investigation meant collecting emails and, occasionally, text messages or Bloomberg terminal chat messages.

But modern business communications now take place over a wide variety of platforms, including applications with private, direct-messaging features, e.g., Slack, Skype, Signal and Telegram, or with ephemeral messaging capabilities designed to delete automatically upon viewing, e.g., Snapchat, Wickr, Dust, Confide, Sicher, Viber and Threema, to name a few.

Reliance on messaging apps to converse about business has become particularly prominent in the current remote working environment, as employees struggle to remain connected — and increasingly use their personal devices to do so.

Despite the growing expectation that companies will either curtail the use of messaging apps for work-related purposes or be prepared to produce data from them in the context of a government investigation, there remains a serious lag in the technology necessary for effective e-discovery of messaging apps — and a dearth of timely or substantive guidance from the U.S. Department of Justice and other government entities on what companies must do to comply with discovery obligations related to them.

While significant attention has been given to the discovery challenges surrounding messaging apps and the ways to mitigate these risks, there is little commentary on how to effectively collect, review and produce data across multiple platforms — including those designed specifically not to be collected — when use of messaging apps are part of a company's culture and its employees' primary method of communicating.

This article offers some practical lessons based on recent experience with such collections and reviews.

Discovery Obligations Related to Messaging Apps

At the outset, it is worth noting that there are many legitimate business reasons to use messaging apps, including those with ephemeral messaging features. Many of these applications offer enhanced security features, such as end-to-end encryption and screenshot protection, which in turn promote compliance with data privacy laws.

Moreover, by automatically deleting messages containing sensitive information, these applications can also reduce the risks and potential costs associated with data breaches.

Applications with ephemeral messaging capabilities can also reduce the burden on companies of hosting and storing large quantities of data. Beyond these practical and cost considerations, many messaging apps are specifically designed to help facilitate collaboration and creativity among employees.

The limited available guidance on the treatment of messaging apps in the context of a government investigation ranges from total prohibition[1] to wavering tolerance for their use. For example, that the DOJ's 2017 guidance on cooperation in Foreign Corrupt Practices Act investigations mandated that companies prohibit employees from "using software that generates but does not appropriately retain business records or communications."[2]

But by 2019, perhaps after realizing the practical limitations on a company's ability to outright prohibit employee use of these applications, the DOJ's guidance now requires only that companies put controls around "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]

Notwithstanding the exponential growth in the number, complexity and popularity of these applications — particularly in startup companies, which are steadily catching the ire of government regulators — neither the DOJ nor any other government agency has released guidance on messaging apps in nearly two years.

Moreover, because the DOJ's existing guidance is broad and forward looking, it offers little meaningful direction on what companies must do if messaging apps were used before controls were implemented, or if a company has made a business judgment to permit the continued use of these applications by employees.

As a result, companies in receipt of a grand jury subpoena or seeking voluntary cooperation credit are faced with the unpleasant decision between devoting significant resources to collecting, reviewing and producing documents from a host of different sources — often at exorbitant costs — without any guidance, or risking being viewed as uncooperative.

Discovery Challenges Involving Messaging Apps

There are a wide variety of discovery challenges presented by messaging apps.

For starters, the data is inherently decentralized in that it often involves communications occurring across multiple platforms — many of which are designed specifically not to be collected — and increasingly on employees' personal devices rather than company devices.

For example, in one recent production in which the authors participated, employees rarely used email to communicate, instead using over 10 different platforms, including Slack, Signal, TeamSpeak, Telegram, WhatsApp, Twitter, LinkedIn, Reddit and Skype.

Moreover, companies — including many founded in the last decade — may not have any headquarters or central severs and may have employees located all over the world. Thus, instead of being able to go into an office to collect from a central data source such as a file or exchange server, company counsel increasingly need to collect data directly from individual employees, and often from their personal devices.

Additionally, because employees often use messaging apps for both professional and personal communications, it can be difficult to ensure collection of only work-related communications. Unsurprisingly, in the context of a criminal investigation, employees can be very reluctant to turn over their personal devices to company counsel for data collection.

Exporting data from messaging apps in a format that is reviewable can also be problematic. Currently, many messaging apps can only be exported in an .xml or .json format, which are dense and difficult to review.

And although many messaging apps allow users to insert documents, pictures and other attachments into the chat, they often cannot be exported in a way that preserves family member information like an email and its attachments. This, in turn, makes it very cumbersome to determine whether exported attachments are responsive and to which portions of the chat they relate.

In addition, because many of these applications are designed to emulate regular conversation, a single chat can be tens of thousands of pages long, switch repeatedly among topics, and contain slang, emojis and other idioms that make review challenging. Moreover, the colloquial nature in which employees converse on messaging apps makes it difficult to develop search terms or use technology-assisted review to identify responsive information.

Together, these challenges make it extremely difficult to predict how long it will take for a company to collect, review and produce documents in a government investigation, where time is typically of the essence.

Lessons Learned

So what is a company facing the prospect of such a daunting undertaking supposed to do?

First, because many of the government policies regarding messaging apps are forward-looking, companies should examine their document-retention policies surrounding them. Businesses that permit the use of messaging apps should assure that any automatic deletion tools are deactivated if their employees are using the application for work-related purposes.

Companies should also consider whether to prohibit the use of messaging apps that have true ephemeral functionality, such as Signal and Wickr, as opposed to ephemeral capabilities that have their own compliance and e-discovery tools to archive messages, such as Slack.

Document-retention policies should also make it clear that if an employee chooses to use a messaging app to conduct business — even on their personal devices — the company has the right to access that data. Additionally, employees should routinely confirm and certify that the deletion tools are inactive on any messaging apps they are using to conduct business.

Second, when faced with the need to collect data from messaging applications, companies should ensure that they fully understand their employees' utilization of messaging apps.

Companies should interview employees to understand (1) all sources of potential data, including all messaging apps that may have been used for work-related purposes; (2) the breakdown of how the employee uses each application for work versus personal communications, as well as the employee's comfort level with potentially collecting personal communications; (3) the employee's phone model, operating system and software version for each messaging app used to conduct business; and (4) the employee's messaging practices, including the use of code words and slang.

Third, companies should develop a detailed plan prior to collection that considers the potential need for tailored solutions depending on employees' devices and messaging app usage. For example, certain phone models and software versions make exporting data from applications extremely cumbersome, or in some instances, impossible. Understanding these types of limitations in advance allows for the development of creative solutions to resolve them before they cause unnecessary delays.

Fourth, in advance of conducting any review, consideration should be given to what will constitute a responsive document for the purpose of each messaging app. For example, in long chat messages, would a responsive document be defined as a single message, a conversation surrounding a certain topic, the relevant conversation plus the surrounding messages for context, or something else?

Companies should also determine whether employees use any slang or code words to reference certain topics and carefully train reviewers on how to identify responsive information based on them.

Fifth, companies should assess their comfort level with producing potentially nonresponsive or privileged information in lieu of conducting a linear review of all chat messages. In order to protect against privilege waiver, companies may also want to consider approaching the government entity or regulator about a nonwaiver agreement or Federal Rule of Evidence 502(d) order.

Finally, counsel for the company should regularly communicate with the government entity or regulator in order to understand their priorities and level-set expectations. Counsel should seek clarification on what custodians and messaging apps the investigators are most interested in and explain any limitations on what the company can provide — e.g., at present, there does not appear to be any way to export data from certain messaging apps.

Conclusion

It is clear that the practice of using messaging apps to conduct business is here to stay. As the number and complexity of these messaging apps continue to proliferate, businesses will need to consider the legal implications of using these applications and develop mechanisms to ensure compliance with discovery demands should they face litigation, or even worse, exposure or involvement in a government investigation.

Jason Weinstein is a partner and Katie Dubyak is an associate at Steptoe & Johnson LLP.

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] See, e.g., Securities and Exchange Commission, Office of Compliance Inspections and Examinations, National Exam Program Risk Alert, Observations from Investment Advisory Examinations Relating to Electronic Messaging (Dec. 2018), available at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf. (directing advisors to prohibit business use of applications that allow employees to "send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back-up").

[2] Dep't of Justice, U.S. Attorney's Manual § 9-47.120(3)(c) (Nov. 2017).

[3] Dep't of Justice, U.S. Attorney's Manual § 9-47.120(3)(c) (Mar. 2019), available at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977. Similarly, in June 2020, the DOJ updated its corporate compliance guidance to emphasize the need for "sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls and transaction." Dep't of Justice, Criminal Division, Evaluation of Corporate Compliance Programs (June 2020), available at https://www.justice.gov/criminal-fraud/page/file/937501/download.