Gov't Scrutiny Of Workplace Chat Apps Set To Keep Growing

By **Jay Williams, Rachel Li Wai Suen and Jackson Hagen** (December 18, 2024)

Jay Williams

Rachel Li Wai Suen

Jackson Hagen

The incoming Trump administration and Republican majorities in Congress are poised to open a variety of investigations after they take power.

Those investigations will most likely follow the recent trend of including demands for people and companies to produce communications made using Slack, Teams and similar workplace chat apps.

On Nov. 14, for instance, Rep. Jim Jordan, R-Ohio, chair of the U.S. House of Representative Judiciary Committee, asked the U.S. Department of Justice's Antitrust Division, the Federal Trade Commission and the U.S. Commodity Futures Trading Commission to preserve materials that include "records created using text messages, phone-based message applications, or encryption software."

It may be a sign of the times — and a preview of what to expect after power changes hands.

More Popular Than Ever

Text and messaging apps are more popular than ever because of the ease and speed of communication they provide.

Yet with that convenience comes increased risk: Employees often fail to consider where these seemingly ephemeral communications may end up. Many do not realize that companies can retain or recover those messages, often with minimal effort.

The apps can also result in employees sending informal and less-than-professional messages.

A lackadaisical attitude to workplace chat apps is a serious risk for any company whose employees use them. That one emoji or unfortunate turn of phrase, especially without context, can come back to haunt an employer should a discovery request or subpoena arrive.

Aggressive Enforcement

In recent years, authorities have aggressively enforced rules requiring companies to retain ephemeral communications.

In one instance, the U.S. Securities and Exchange Commission settled with 16 banking firms that paid combined penalties of over $1.1 billion to resolve allegations they violated recordkeeping requirements.

In that case, employees "routinely communicated about business matters using text

messaging applications on their personal devices," and "[t]he firms did not maintain or preserve the substantial majority of these off-channel communications."[1]

The SEC settled similar charges in August with 26 companies that agreed to pay nearly $393 million in penalties.[2]

Similar issues have arisen in recent high-profile criminal prosecutions. For instance, in the September indictment of New York Mayor Eric Adams in the U.S. District Court for the Southern District of New York, the government alleged that Adams "assured [a] Staffer that he had a practice of deleting all his messages with" the staffer, purportedly as part of a series of actions to conceal his conduct.[3]

Text messages between former Sen. Bob Menendez, D-N.J., and his wife also were heavily featured at his trial on bribery charges earlier this year, also in the Southern District of New York.[4]

Growing Scrutiny

A series of statements from various agencies underscores the government's interest in these kinds of communications.

In January, updated guidance from the DOJ and FTC warned of the need to preserve documents, including "data from ephemeral messaging applications designed to hide evidence."[5]

And recent updates to corporate compliance memos from the DOJ's Antitrust[6] and Criminal[7] Divisions emphasized that the DOJ would consider policies regarding the use of messaging apps in evaluating compliance programs.

Members of Congress and the Trump administration have expressed an interest in investigating companies and individuals, as well — to say nothing of the investigative powers of agencies such as the DOJ, FTC, SEC and Consumer Financial Protection Bureau.

Shortly before the election, the House Committee on Oversight and Accountability sent a request to NewsGuard — a company that provides a rating system for news websites and provides misinformation tracking and brand safety services, among other things — for documents and communications.[8]

The request stemmed from the committee's investigation into whether the company is a "non-transparent agent of censorship campaigns" and into "abuse of government authority to censor American citizens."

After the election, several House committees asked the U.S. Department of Labor to preserve communications relevant to the committees' ongoing investigations into the Biden administration, including those related to border policy, the withdrawal from Afghanistan and other items.

The request signaled that the House will continue to aggressively investigate the Biden administration across a range of issues implicating the private sector, including, as the letter to the DOL noted, whether the administration "collu[ded] with social media companies to suppress free speech."[9]

President-elect Donald Trump, individuals he plans to nominate for key federal agency

leadership roles, and incoming and current members of Congress have suggested that these types of investigations will be the norm, particularly at the outset of the new administration.

What Companies Should Consider Doing

Given the increasing scrutiny, companies should evaluate usage and retention policies, especially as they relate to app-based communications.

For example, what is the current retention period for messaging apps? If these apps are meant for fleeting or temporary conversations, messages should be retained for a very short period to reinforce that position, as well as to minimize risk and data storage costs. A retention period of 90 days or even 30 days, with no archive, is reasonable and defensible for messaging apps that are not intended to contain important business information.

Companies also should educate employees about using these apps and set explicit expectations in their policies.

The Need for a Communication Policy

A communications policy should state clearly what messaging apps are approved for use — and that other applications are not approved and should not be used — and how such apps should be used.

The policy should ensure that employees understand that these applications are not the place to discuss anything substantive, and that their use should always be professional. It never hurts to tell employees that the company can view messages and will discipline employees who misuse the apps.

Companies should evaluate these policies regularly and refresh them as needed. They also should train employees on them at a regular cadence, similar to annual ethics and compliance training.

Companies should also enforce the policies — they lose much of their effectiveness if they are not acted upon. In fact, a court may find that having a retention policy but not enforcing it shows bad faith on the part of the company.[10] The DOJ likely would come to a similar conclusion.

Companies should set up automatic deletion and archiving procedures to ensure that once they set a retention policy, they apply it consistently.

An Obligation to Retain

Companies also should be able to quickly suspend deletion practices when a legal obligation to retain is triggered.

This is critical for all document types, but companies should pay particular attention to messaging apps. Changing retention and deletion policies in those applications may be more complicated or difficult than in traditional document management systems.

In addition, these types of applications are often not considered, or are considered much too late, when litigation holds are put in place. Even with a strict and short retention period, companies can face criticism for not retaining the 30- or 90-days' worth of messages when a subpoena or litigation demand arrives.

Slack, Teams and messaging apps like WhatsApp appear here to stay. They help employees connect and communicate with ease, but it is important to consider the risks that come with using such apps in the workplace — risks that only show signs of growing.

Jay Williams is a partner, Rachel Li Wai Suen is senior counsel and Jackson Hagen is a managing associate at Orrick Herrington & Sutcliffe LLP.

[1] https://www.sec.gov/newsroom/press-releases/2022-174.

[2] https://www.sec.gov/newsroom/press-releases/2024-98.

[3] https://www.justice.gov/d9/2024-09/u.s._v._adams_indictment_1.pdf.

[4] https://www.nytimes.com/2024/05/28/nyregion/bob-nadine-menendez-text-messages.html.

[5] https://www.justice.gov/opa/pr/justice-department-and-ftc-update-guidance-reinforces-parties-preservation-obligations.

[6] https://www.justice.gov/d9/2024-11/DOJ%20Antitrust%20Division%20ECCP%20-%20November%202024%20Updates%20-%20FINAL.pdf.

[7] https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl.

[8] https://oversight.house.gov/wp-content/uploads/2024/10/Newsguard-Followup-Request_10.25.2411.pdf.

[9] https://mikejohnson.house.gov/news/documentsingle.aspx?DocumentID=1477.

[10] See Micron Tech., Inc. v. Rambus Inc., 917 F. Supp. 2d 300, 316 (D. Del. 2013). In this case — a civil patent lawsuit — a court found that a party's spoilation of evidence was done in bad faith, in part due to its "selective enforcement" of its document retention policy.