COSMOS
Navigate the Compliance Universe

CEP Magazine - October 2023

Kurt Gottschall (kurt.gottschall@haynesboone.com) is a Partner at Haynes Boone in Denver, Colorado, USA.

Timothy Newman (timothy.newman@haynesboone.com) is a Partner at Haynes Boone in Dallas, Texas, USA.

Payton Roberts (payton.roberts@haynesboone.com) is an Associate at Haynes Boone in Dallas, Texas, USA.

What to do about business-related text and WhatsApp messages

By Kurt Gottschall, Timothy Newman, and Payton Roberts

Over the past year, US financial regulators have announced game-changing enforcement cases and corporate cooperation guidelines to prompt businesses to retain, review, and—if subpoenaed—produce employees' business-related text messages on both personal devices and within so-called ephemeral messaging apps such as WhatsApp, Snapchat, Telegram, Confide, and many others. The ephemeral apps are particularly ubiquitous, and many employees mistakenly believe that their messages will disappear almost magically, leaving no trace. But the technical reality is not that simple, presenting innumerable challenges for legal and compliance staff. This article highlights the recent regulatory scrutiny concerning messaging and offers practical considerations for companies of all sizes.

Recent regulatory enforcement and policy guidance

As we described in our Off-Channel Communications Client Alert,[1] in September 2022, the U.S. Securities and Exchange Commission (SEC) and Commodity Futures Trading Commission (CFTC) filed 16 enforcement actions against some of the nation's largest financial firms for not preserving or reviewing text or ephemeral messages.[2] In these cases, regulators imposed more than $2 billion in penalties, required admissions, and ordered significant remedial undertakings.[3] Regulators brought these cases based upon the statutory obligations of broker–dealers, investment advisers, and commodity pool operators to preserve certain documents for inspection and review business communications as part of their routine supervision of employees.[4]

More recently, on May 11, 2023, the SEC announced settled enforcement actions against two additional broker–dealers that self-reported their failure to preserve and review off-channel communications: HSBC Securities Inc. and Scotia Capital Inc.[5] In announcing the actions, Gurbir Grewal, the director of the SEC's Division of Enforcement, encouraged other broker–dealers to self-report and noted that both firms received "reduced penalties [because of] their efforts and cooperation."[6] The SEC imposed civil penalties against HSBC and Scotia Capital of $15 million and $7.5 million, respectively—which were approximately 5%–12% of the top-tiered penalties of $125 million paid by some of the largest Wall Street firms.

Although public companies are not subject to the specific document preservation and employee supervision requirements imposed on SEC and CFTC registrants, both the U.S. Department of Justice (DOJ) and the SEC have communicated their expectations regarding messaging preservation. In 2021, Grewal noted that failing to preserve business-related text messages may "obstruct investigations, [and] raise broader accountability, integrity and spoliation issues."[7] Grewal later warned that:

> "[SEC enforcement will] consider all of our options when this sort of misconduct occurs prior to or during our investigations. For example, if we learn that, while litigation is anticipated or pending, corporations or individuals have not followed the rules and maintained required communications, have ignored subpoenas or litigation hold notices, or have deliberately used the sort of ephemeral technology that allows messages to disappear, we may well conclude that spoliation of evidence has occurred and ask the court for adverse inferences or other appropriate relief."[8]

The SEC described the "likely" impact on its enforcement investigations in bringing each of the 16 settled enforcement actions against Wall Street firms for not preserving or reviewing text or ephemeral messages as follows:

> "During the time period that Respondent failed to maintain and preserve offchannel communications its employees sent and received related to the broker-dealer's business, [Respondent] received and responded to Commission subpoenas for documents and records requests in numerous Commission investigations. As a result, [Respondent]'s recordkeeping failures likely impacted the Commission's ability to carry out its regulatory functions and investigate violations of the federal securities laws across these investigations."[9]

DOJ has communicated its focus on text messages and ephemeral communications by announcing a series of significant modifications to its published policies for evaluating corporate cooperation and compliance programs. This guidance is important because DOJ prosecutors across the country are required to consider it in evaluating any corporate settlement or declination of prosecution.

Specifically, DOJ has rolled out three recent policy announcements touching on messaging. In September 2022, Deputy Attorney General Lisa O. Monaco announced that going forward, in evaluating compliance programs, DOJ's Criminal Division would consider whether companies maintained "effective policies governing the use of personal devices and third-party messaging platforms for corporate communications."[10] DOJ further directed prosecutors to "consider whether a corporation seeking cooperation credit in connection with an investigation has instituted policies to ensure that it will be able to collect and provide to the government all non-privileged responsive documents relevant to the investigation, including work-related communications (*e.g.*, texts, e-messages, or chats), and data collected on phones, tablets or other devices that are used by its employees for business purposes." In December 2022, a speech by another senior DOJ official recognized that while there may be legitimate reasons for employees to use ephemeral messaging, these apps present significant challenges to a company's ability to both ensure that it has a well-functioning compliance program and also to access those communications when required. DOJ also announced that in some cases, the Criminal Division would require CEOs and chief compliance officers to certify that the company maintained a well-functioning compliance program and had access to required business communications.[11]

In March 2023, DOJ's Criminal Division announced even more prescriptive guidance concerning both text and

ephemeral messaging in revisions to DOJ's *Evaluation of Corporate Compliance Programs* (ECCP).[12] Under the revised ECCP, DOJ will now consider:

- Each company's specific risk profile, and whether their policies ensure that, "to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company";
- Hardware policies, including "bring your own device" programs and associated preservation policies;
- Approved electronic messaging applications for business communications, including preservation and deletion settings;
- The communication of messaging application policies to employees; and
- Whether company compensation structures include positive incentives such as career advancement or monetary rewards for developing, improving, or meeting established compliance standards, impose financial penalties for misconduct or failure to comply with corporate compliance policies, and whether such policies are enforced on a consistent basis.

In rolling out the ECCP revisions, a senior DOJ official further announced that "[d]uring the investigation, if a company has not produced communications from these third-party messaging applications, our prosecutors will not accept that at face value."[13] Instead, when a company fails to produce such communications, prosecutors will further scrutinize the company's ability to access those communications, how they are stored, and "a company's answers—or lack of answers—may very well affect the offer it receives to resolve criminal liability."

Proactive guidance for public companies

Preserving and reviewing employees' business-related communications on personal devices and messaging apps can feel like navigating a minefield of criminal and civil document preservation obligations, employee privacy considerations, and technological/resource challenges. While financial regulators have been slow to articulate practical expectations to issuers, the recent SEC enforcement actions and prescriptive guidance from DOJ provide a roadmap of key areas for companies to develop or revisit relevant policies and procedures. After refining these policies, it is equally important for issuers to update and test their effectiveness regularly.

Hardware policies

In the past, many organizations adopted bring-your-own-device (BYOD) policies for employees because it was cheaper than providing employees with a separate work phone, eliminating the hassle of carrying two phones. When companies opt for BYOD, their written policies and procedures should include, at a minimum: (i) clear delineation of approved and disapproved messaging apps for business communications; (ii) guidelines specifying what constitutes business communications versus personal communications on BYOD devices; and (iii) employee acknowledgement that as a condition of receiving reimbursement of all or part of their BYOD expense, business-related communications are the property of the company and subject to the company's existing retention protocols (outlined more below).

On the other hand, mandating that employees carry and use only company-owned devices (COD) for business communications often is more expensive, and employees may be resistant to carrying a second phone and never using personal phones for business communications. In today's business world, where friendships and business relationships often coincide, it can be awkward for employees to decide how to respond when they receive business-related messages on their personal devices or unapproved apps. Therefore, COD policies should provide

specific instructions and procedures for moving business communications from a personal device to a company device to comply with existing retention policies.

App policies

Ephemeral messaging applications continue to evolve rapidly, with new apps constantly claiming better encryption and automatic message deletion technologies. Therefore, it is imperative to clearly define approved apps while making clear that new or unlisted apps are prohibited absent explicit corporate approval. In determining approved messaging apps, IT and compliance staff must fully understand the functionality of each app and its compatibility with existing company archiving vendors and requirements. The primary feature of many messaging apps—automatic destruction of messages—should be prohibited. Because it is impractical for companies to review and archive personal email accounts, many companies also prohibit the use of personal email for business communications. Companies should consider third-party management (outlined later) of app and email retention, which in turn may impact their policies for approved messaging apps and personal email platforms.

Social media policies

Like ephemeral messaging apps, employee use of social media can present compliance challenges because the dividing line between business and personal communications can be murky, and the messaging features of many apps can be difficult to archive and review. As with ephemeral messaging apps, it's critical to differentiate between approved and unapproved social media sites for business-related communications. Many companies approve of LinkedIn and similar business networking sites while strongly discouraging or prohibiting business communications on social media channels more associated with personal lives, such as Facebook and Instagram. Companies also should determine whether to conduct or outsource surveillance of publicly facing social media for impermissible uses.

Retention/archiving systems and policies

Due to increased regulatory scrutiny on messaging, many outside vendors are launching new and less expensive products with customized features designed to capture, archive, and enable the review of vast numbers of electronic communications. Following vendor and platform selection, policies and procedures should contain specifics regarding how employees interact with the system, including defining employee preservation obligations, deletion options, and the process for obtaining exceptions from default settings. Typically, written policies should also spell out aggregate firm document retention policies and establish protocols for system testing, data recovery, and resilience.

Company control and review protocols

Unfortunately, responsibilities to messaging do not end with capture and archiving. Regulators also expect companies to develop and implement protocols for both periodic and event-driven reviews. For routine, periodic review of electronic communications, written policies should require preapproval by technology or compliance staff, designate review frequency, designate responsible staff or a third party, and define a process for determining/revising automated search terms. These steps are especially significant under a BYOD program. Among other things, companies should consider loading security applications or other software to implement cybersecurity protections, monitor for prohibited applications, and "wipe" the device if lost or stolen. It is vital to reassess the efficacy of review policies at least annually as technology and terminology evolve. To the extent practicable, it is also advantageous to consider protocols governing additional document preservation and review to be conducted in response to specific events such as the commencement of internal investigations,

whistleblower complaints, government investigations, or private litigation. By considering these scenarios ahead of time, compliance staff have time to think through potential pitfalls, such as dotted-line employee supervisory relationships that may impact document collection obligations.

Employee training and attestations

Ultimately, no organization will be successful in preserving employees' business-related messages unless the employees are well-trained and cooperative. Tellingly, all the Wall Street firms charged by the SEC and CFTC had policies and procedures governing approved and unapproved business communications channels; however, the firms failed to implement sufficient systems to ensure employees at all seniority levels followed those policies. Given financial regulators' recent focus on the issue, we recommend that employee training:

- Occur at onboarding, periodically (at least annually or through regular reminders), and during offboarding (e.g., to ensure that business-related communications are collected from personal devices prior to employee departure);
- Clearly defines that business-related messaging is allowable *only* on preapproved apps and personal devices;
- Describes company protocols for future review and data collection from employees' personal devices;
- Provides practical guidance for how to respond when third parties communicate with employees on unapproved channels (e.g., moving communications to approved channels and/or expectations for belated preservation/archiving); and
- Explains procedures for self-reporting possible violations of firm policies, hotline or other anonymous reporting mechanisms, and related disciplinary policies.

Periodic employee attestations present an additional administrative burden but can be important in demonstrating an appropriate compliance environment to regulators. We recommend that companies obtain attestations during onboarding, offboarding, and at least annually during employment. Typically, attestations should include affirmative representations that employees know and understand messaging policies and have only used approved apps and business email accounts or preserved unsolicited communications from third parties on unapproved apps or channels.

Senior management messaging

In a multitude of recent speeches and policy pronouncements, regulators have made clear that their evaluation of corporate compliance programs includes an assessment of the tone at the top. The well-publicized DOJ policy announcements and SEC/CFTC enforcement cases regarding messaging provide an easy entrée for senior management to communicate their organization's commitment to compliance in this area by announcing new or refined policies, sending periodic emails to all staff or providing relevant training.

Compliance incentives and disciplinary actions

Recognizing that employee compliance with messaging policies is essential, both DOJ and the SEC have taken steps to prompt issuers to maintain robust incentive and disciplinary frameworks. For example, the settled SEC enforcement actions required that each of the 16 Wall Street firms retain an independent compliance consultant to recommend disciplinary frameworks for noncompliance with messaging policies that included corrective actions, graduating levels of discipline, and the consistent application of disciplinary policies across business

units and levels of seniority. In evaluating corporate cooperation and compliance environments, both DOJ and the SEC have urged issuers to provide compensation and career advancement incentives for compliance and meaningful sanctions for noncompliance, including compensation penalties—for egregious or repeated violations—and termination.

Proactive planning for e-discovery

Many government investigations arise unexpectedly, and it can be very demanding to provide rapid and fulsome responses to subpoenas that call for producing a wide variety of electronic communications. To prepare for these contingencies, we recommend proactively mapping how each employee's electronic data (including emails, texts, and other messages) is stored on company or third-party servers or backup systems. Proactively considering this storage can help issuers identify and fix retention gaps and develop more efficient e-discovery procedures (e.g., limiting the number of servers that need access and searching for certain business units). We recommend that issuers develop document preservation (i.e., hold notice) templates to send to employees in response to government investigations or threatened private litigation. Issuers should also have IT professionals consider chain of custody, the preservation of metadata, and the compatibility of electronic messaging collection/archiving systems with selected e-discovery and document review platforms. Proactively verifying compatibility can help issuers avoid costly data conversions during e-discovery.

Contract with a software vendor

Though often expensive, third-party vendors may alleviate additional burdens on current staff while helping to ensure compliance with business communication retention and review policies. The SEC Examination staff has recommended the use of outside software vendors, through company-approved software or applications under either BYOD or COD programs, to: "(i) monitor the social media posts, emails, or websites, (ii) archive such business communications to ensure compliance with record retention rules, and (iii) ensure that they have the capability to identify any changes to content and compare postings to a lexicon of key words and phrases."[14] A software vendor can also set up automatic alerts triggered by communications in violation of company policies. To avoid privacy concerns related to such monitoring, company policies should prohibit using personal social media or messaging for business communications and clarify that business-related messages are the company's property.

Takeaways

- The U.S. Securities and Exchange Commission's scrutiny of text and ephemeral messaging retention programs is expanding to all entities under their purview.
- The U.S. Department of Justice has provided explicit guidance that federal prosecutors will consider the effective retention of text and ephemeral messages in evaluating corporate compliance programs and cooperation in their investigations.
- In reevaluating policies for retention of text and ephemeral messages, companies need to consider costs and balance compliance with employee privacy.
- Companies need to understand the full functionality of employee mobile devices, apps, and social media outlets to develop credible retention programs.
- A policy is only as effective as its implementation and enforcement measures. Implementation should include annual training, periodic messaging from senior management regarding compliance, and the consistent application of disciplinary measures for violations of retention policies.

1 Kit Addleman, Kurt Gottschall, and Timothy Newman, "SEC and CFTC Send $2 Billion Message Regarding Monitoring and Preserving Employee Electronic Communications," Hayes Boone, October 19, 2022, https://www.haynesboone.com/news/alerts/sec-and-cftc-send-$2-billion-message.
2 U.S. Securities and Exchange Commission, "SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures," news release, September 27, 2022, https://www.sec.gov/news/press-release/2022-174.
3 Securities and Exchange Commission, "SEC Charges 16 Wall Street Firms."
4 17 C.F.R. § 240.17a-4(b)(4) of the Securities Exchange Act of 1934; 17 C.F.R. § 275.204-2(a)(7) of the Investment Advisers Act of 1940; and 7 U.S.C. § 6s(f)(1)(C), 7 U.S.C. § 6s(g)(1) and 7 U.S.C. § 6s(g)(3), and 7 U.S.C. § 6s(h)(1)(B) of the Commodity Exchange Act.
5 U.S. Securities and Exchange Commission, "SEC Charges HSBC and Scotia Capital with Widespread Recordkeeping Failures," news release, May 11, 2023, https://www.sec.gov/news/press-release/2023-91.
6 Securities and Exchange Commission, "SEC Charges HSBC and Scotia Capital."
7 Gurbir S. Grewal, "PLI Broker/Dealer Regulation and Enforcement 2021," transcript of a speech delivered in Washington, DC, October 6, 2021, https://www.sec.gov/news/speech/grewal-pli-broker-dealer-regulation-and-enforcement-100621.
8 Gurbir S. Grewal, "Remarks at SEC Speaks 2021," transcript of a speech delivered in Washington, DC, October 13, 2021, https://www.sec.gov/news/speech/grewal-sec-speaks-101321.
9 Securities and Exchange Commission, "SEC Charges 16 Wall Street Firms."
10 Lisa O. Monaco, "Memorandum Concerning Further Revisions to Corporate Enforcement Policies Following Discussions with Corporate Crime Advisory Group," September 15, 2022, https://www.justice.gov/opa/speech/file/1535301/download.
11 Nicole M. Argentieri, "Acting Principal Deputy Assistant Attorney General Nicole M. Argentieri Delivers Remarks at the 39th International Conference on the Foreign Corrupt Practices Act," transcript of a speech delivered in Washington, DC, December 1, 2022, https://www.justice.gov/opa/speech/acting-principal-deputy-assistant-attorney-general-nicole-m-argentieri-delivers-remarks.
12 U.S. Department of Justice, Criminal Division, *Evaluation of Corporate Compliance Programs*, March 2023, https://www.justice.gov/opa/speech/file/1571911/download.
13 Kenneth A. Polite Jr., "Assistant Attorney General Kenneth A. Polite, Jr. Delivers Keynote at the ABA's 38th Annual National Institute on White Collar Crime," transcript of a speech delivered in Miami, FL, March 3, 2023, https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-keynote-aba-s-38th-annual-national.
14 U.S. Securities and Exchange Commission, "Observations from Investment Adviser Examinations Relating to Electronic Messaging," December 14, 2018, https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf.