CEP Magazine - January 2021
Balancing effective compliance policies against the ubiquity of ephemeral messaging

By Daniel J. Polatsek

Daniel J. Polatsek (daniel.polatsek@icemiller.com) is a Chicago-based partner in Ice Miller's White Collar Defense and Investigations Groups, where he oversees internal investigations and handles sensitive corporate governance and litigation matters for both public and private companies.

As we enter into the first quarter of 2021, the available evidence indicates that remote work is going to remain part of the work-life balance for much of this year. The US workforce continues to face unexpected pay cuts, furloughs, and layoffs, while senior executive teams and upper management face pressures to meet revenue expectations and budgeted projections for both shareholders and Wall Street.

For many companies, these economic pressures require reductions in force, consolidating greater authority within a smaller workforce and executives who have less time to supervise and approve operational decisions. The dilemma now is how the private sector responds to the challenge of having to do more with less but just as fast.

The answer, in part, is better, faster, and more secure communication platforms, but the technologies that make speed and efficiency possible, such as ephemeral messaging (i.e., mobile-to-mobile transmissions that are designed to self-delete from the recipient's screen after the message has been viewed) and employee use of personal devices for business, raise complicated issues for compliance departments seeking to manage risk without overmanaging business solutions that allow companies to stay productive.

Compliance programs in the pandemic

Over the past year, the Department of Justice has made clear that the pandemic will not excuse a substandard compliance infrastructure.[1] Companies are still required to tailor compliance programs designed to prevent, detect, and remediate unlawful conduct. This was most recently discussed in the virtual town hall held by representatives of the Department of Justice, the Securities and Exchange Commission, and the Federal Bureau of Investigation on May 20, 2020. These agencies made clear that while the pandemic is a challenging environment for compliance programs, the pandemic is not a defense to inadequate compliance protocols resulting in unlawful conduct.[2] Following the virtual town hall this past May, the Department of Justice also issued its updated *Evaluation of Corporate Compliance Programs* guidance in June 2020.[3] The guidance touched upon several different factors necessary for an effective compliance program. One key takeaway was that an organization's compliance program must be rationally tailored to the risks inherent to that organization's business operations. Put another way, *how and why* a company designed its compliance program can be an important factor in whether the company is afforded leniency later by a regulator if one or more of its employees is involved in unlawful conduct.

The necessity of internal investigations

If the past is prologue, companies will continue to have to investigate civil and criminal conduct such as conflict

of interest schemes, trade secret misappropriation, public corruption, price fixing, embezzlement, and insider trading, to name a few. Each scheme dictates its own appropriate investigatory methodology and constituent audiences, but the objectives remain the same: stop potential unlawful conduct, understand the nature and extent of the unlawful conduct, lawfully mitigate the legal and business risks arising from the unlawful conduct, and prevent the same or similar unlawful conduct from reoccurring. Meeting the foregoing objectives during an internal investigation is accomplished through an examination of the available evidence that generally hails from two sources: (1) witness interviews and (2) documentary evidence (i.e., electronic and hard-copy documents and communications). When witnesses cannot or will not fill in the details of a fraud scheme or other unlawful conduct, transactional records, hard-copy documents, and electronic communications are critical to filling in the information gaps.

Those overseeing an internal investigation, such as in-house counsel, audit committees, boards of directors, and other authorized stakeholders, must frequently assess whether the current circumstances warrant voluntary disclosure of the conduct being investigated to a regulator. Among other important considerations is whether a company's voluntary disclosure would allow it to seek leniency; cooperation credit; or, in a best case scenario, avoid any adverse consequence all together. The extent to which a company may be extended leniency within the context of a voluntary disclosure can be linked, in part, to its own root cause analysis of the underlying unlawful conduct. In other words, the degree to which leniency is extended to a company may be contingent on the company's efforts to understand the who, what, where, when, and how behind the unlawful conduct being investigated. Stated differently, corporate leniency extended by a regulator may be measured, in part, by how much a company can inform the government about what happened.

Once a voluntary disclosure is made and leniency is sought through cooperation credit or another avenue, it should be anticipated that a company's compliance program will be evaluated with respect to its capabilities to prevent and detect unlawful conduct through its preexisting compliance policies. Because ephemeral messaging is quickly becoming an integral part of how employees in corporate America communicate, companies can expect regulators to inquire about ephemeral messaging, the compliance policies underlying its use, and the policies underlying its preservation and collection during an investigation.

Challenges posed by ephemeral messaging

Although there are several different forms of ephemeral messaging that appear through social media and work-related platforms (e.g., Snapchat, WhatsApp, Wickr), the common denominator to all of these applications is the self-delete function after the communication is opened and read by the recipient. Because these communications are designed to be peer-to-peer communications, they generally do not travel through employer servers and are oftentimes encrypted, making the recovery of these communications by a private employer extraordinarily difficult if not impossible without prior protocols in place.

The value to ephemeral messaging is found in its speed, efficiency, and security. Unlike email, ephemeral messaging is very similar to having a brief in-person conversation that allows you to get to the point quickly and avoids the exchange of time-consuming formalities of an in-person conversation. Ephemeral messaging also allows the sender to entertain multiple different conversations at once. Another benefit to ephemeral messaging is the security found in its end-to-end encryption, which is useful when sensitive, proprietary, or other confidential business information must be discussed in real time. It is also attractive given the proclivity of malware, ransomware, and other types of data breaches targeting the private sector.

But the very same things that make ephemeral messaging an attractive form of communication can become critical gaps in a company's compliance infrastructure. Specifically, ephemeral messaging is a particularly good tool for concealing unlawful conduct because it is exceptionally difficult to monitor or recover these

communications. As a result, should ephemeral messaging serve as the primary form of communication in perpetrating an unlawful activity, it is possible that, without the right protections, a thorough internal investigation and root cause analysis cannot be adequately performed—meaning, potentially unlawful conduct cannot be remediated as quickly or as fully as it may have otherwise been—and this compliance gap could potentially interfere with the degree of leniency or cooperation credit granted to a company by a regulator when a voluntary disclosure is made. Depending on the size and scale of the unlawful conduct at issue, the consequences could be very impactful.

In *A Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition* , the Department of Justice states part of obtaining leniency for the commission of unlawful conduct involving violations of the Foreign Corrupt Practices Act (FCPA) must include a thorough analysis of causes of the underlying unlawful conduct with a goal of timely and appropriately remediating those causes to prevent similar misconduct from occurring again.[4] It is also expressly stated that companies seeking leniency for FCPA violations must implement appropriate guidance and controls on the use of ephemeral messaging applications that could undermine a company's ability to retain business records or communications or otherwise comply with the company's document retention policies or legal obligations. While not as explicit in its policy pronouncements, the Antitrust Division of the Department of Justice has made it clear that it will be looking at whether a company's compliance policies are designed to address not only the technical changes regarding a company's business operations, but whether its compliance policies are also designed to address new methods of electronic communications that are being used and if those methods increase the risk of antitrust violations or undermine preexisting compliance policies.

What the foregoing makes clear is that there is an expectation from at least some divisions within the Department of Justice that compliance policies should be proactively managing the risks technologies like ephemeral messaging pose, such that its use will not allow it to be used to exploit unlawful purposes or unduly interfere with a company's ability to perform an adequate root cause analysis. A fair inference from the foregoing is that regulators will view ephemeral messaging as business records similar to other communications or documents that must be maintained, preserved, or recovered as part of an internal investigation or response to a grand jury subpoena.

Companies that support the widespread use of ephemeral messaging but do not take proactive steps to address or mitigate the risks in employing this communication platform may be viewed skeptically or, in a worst case scenario, willfully blind if the failure to address this type of communication platform is conspicuously absent. This would seem particularly true for companies where bid rigging, bribery, price fixing, or FCPA violations are a concern.

Compliance options

Because the potential consequences of serious unlawful conduct can be transformational with respect to stakeholder relationships, reputation, and civil and criminal enforcement, it makes sense for compliance departments to address the use of ephemeral messaging head-on. A starting point can be the rapport between compliance personnel and senior management. Understanding how and why ephemeral messaging is used and by whom within the organization will illustrate why it is important and where the greatest risks lie. Memorializing this internal risk assessment can explain how and why certain decisions were made about the compliance policies governing the permissible uses of ephemeral messaging. Put another way, a company can set forth the basis of the business justification for using ephemeral messaging and why its use makes sense within the context of the risks it poses to a compliance program.

For example, access to ephemeral messaging might have a number of valid business reasons for a manufacturer with international clients, but where outside consultants or other third-party intermediaries are used

internationally or where foreign governmental approval is required, such use of ephemeral messaging would warrant careful scrutiny. Therefore, with respect to ephemeral messaging, compliance programs can provide guidance on:

- The types of information that can and cannot be transmitted through ephemeral messaging.
- Which persons within the company are specifically authorized to use ephemeral messaging and those who are not, and
- The types of work-related communications that are prohibited for this communication platform.

Consideration can also be given to tailoring in-person training and/or narrowly tailored Webex module training to ensure each individual authorized to use ephemeral messaging does so in a manner consistent with company policy. In this way, ephemeral messaging is not unlike other important compliance policies governing the receipt or use of gratuities, reimbursable business development expenses, and appropriate political contributions.

On an enterprise level, the compliance department can partner with the information technology department to understand available options that allow internal ephemeral messaging without sacrificing record retention. At a minimum, this partnership can develop internal protocols to suspend the use of ephemeral messaging in the event unlawful conduct is discovered, investigated, or must be voluntarily disclosed to law enforcement. Litigation hold notices should also explain how a litigation hold affects individual use of ephemeral messaging.

Other controls can include policies that prohibit using ephemeral messaging with external business partners or using software that allows only company-sanctioned ephemeral messaging applications to be downloaded on employer-issued mobile devices or computers.

Unique challenges of personal mobile devices

Companies should anticipate that employees will use their personal mobile devices for work, which includes the use of ephemeral messaging. As a result, guidance on what applications and what content are permissible for conducting work-related communications on a personal mobile device should be given similar to that of other company policies governing the use of ephemeral messaging. Where company-issued mobile devices are issued to employees, companies can install mobile management software for monitoring employee communications and publish an express list of prohibited applications that cannot be used to conduct company business.

Because personal mobile devices contain both personal information and business-related communications, they can be particularly vexing from a compliance standpoint. Therefore, companies are well advised to have an express policy mandating employees read, certify, and consent to a policy that includes some or all of the following:

- If company business is conducted on a personal mobile device, an employee cannot later deny that employer access to the business-related data stored on that device.
- That the employee understands they have no expectation of privacy in the work-related content on a personal mobile device.
- That the employee further agrees that the user's work-related content may be monitored, reviewed, copied, and disclosed without the consent or approval of the employee at the employer's discretion.

This same message should be reiterated in the company employee handbook and, where required, posted on internal bulletin boards.

Ensure your program is taking ephemeral messing into account

While not easy, compliance solutions exist for navigating the use of ephemeral messaging and the use of personal devices in a remote work environment. Even in a remote work environment, during an extended pandemic, be proactive in understanding how and why ephemeral messaging is needed and used, and the unique risks to the company.

The opinions expressed are those of the author alone and do not reflect the view of the Ice Miller LLP. This article is for general information purposes only and is not intended to be and should not be taken as legal advice.

Takeaways

- Communication between compliance personnel and management should be established to assess the utility and risk of the use of ephemeral messaging and personal mobile devices.
- Internally memorialize the business justification for using ephemeral messaging and personal mobile devices within the context of the risks.
- In-person and webinar training on the permissible and prohibited uses of ephemeral messaging and personal mobile devices for company business should be considered.
- Compliance departments should partner with information technology to understand the capabilities of its own record retention and ability to suspend ephemeral messaging for an investigation.
- Companies should have an express privacy policy mandating employees' consent to the company's monitoring and collection of ephemeral messages and company communications on personal devices.

1 U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated June 2020), http://bit.ly/2Z2Dp8R.
2 Timothy D. Belevetz, Guillermo Christensen, Daniel Polatsek, and Meredith Wood, "DOJ, SEC & FBI Host Virtual Town Hall on Foreign Bribery and Health Care Fraud Enforcement," Ice Miller, May 21, 2020, https://bit.ly/32u6Btx.
3 U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs*.
4 U.S. Dep't of Justice and the Enforcement Div. of the U.S. Securities and Exchange Comm'n, *Resource Guide to the U.S. Foreign Corrupt Practices Act, Second Edition*, July 2020, https://bit.ly/2FBw5g7.