Cooley

Considering Texting About Work? Beware.

January 24, 2023

As the rise in remote work has led to an increased reliance on mobile devices to stay connected – with cellphones at our fingertips virtually 24/7 – the use of third-party messaging applications to communicate about work has become commonplace. From WhatsApp to Telegram, corporate executives, financial services professionals and other employees around the globe routinely communicate about their businesses using messaging applications that are not tied to their corporate systems. This practice presents an array of compliance-related challenges for employers that have often been ignored, and law enforcement and regulatory agencies have taken notice.

In fall 2022, the US Department of Justice clearly signaled that it is cracking down on workplace use of personal devices and third-party messaging applications. On September 15, DOJ Deputy Attorney General Lisa Monaco issued a memo detailing revisions to the DOJ's corporate criminal enforcement policies. Among other things, the memo focuses on corporate compliance programs and, notably, companies' ability to monitor employee use of personal devices and third-party apps:

> *The ubiquity of personal smartphones, tablets, laptops, and other devices poses significant corporate compliance risks, particularly as to the ability of companies to monitor the use of such devices for misconduct and to recover relevant data from them during a subsequent investigation. The rise in use of third-party messaging platforms, including the use of ephemeral and encrypted messaging applications, poses a similar challenge.*

The memo makes clear that in evaluating the effectiveness of a corporate compliance program and in assessing a corporation's cooperation in an investigation, the DOJ will consider a corporation's policies and procedures governing the use of personal devices and messaging platforms for business communications. The memo also previewed that additional guidance on best practices would be forthcoming.

In mid-October 2022, the DOJ announced a $778 million plea deal by Lafarge, a French industrial company and the world's largest cement manufacturer, for conspiring to support terrorist organizations. Referencing the September 2022 policy memo, Monaco addressed the role that off-channel electronic communications played in the investigation:

> *We also emphasize that companies should have policies to enable retention and production of communications over third-party messaging systems. Lafarge did not. Nonetheless, thanks to the efforts and ingenuity of our agents and prosecutors, we were able to locate the inculpatory emails that Lafarge executives tried to hide off-system.*

For financial services firms that are registered with the Securities and Exchange Commission and thus subject to the SEC's record-keeping rules, the stakes can be even higher. For example, in September 2022, the SEC announced a more than $1.1 billion resolution of an investigation involving 15 broker-dealers and one affiliated investment adviser and failures to maintain and preserve electronic communications in violation of certain record-keeping provisions in the federal securities laws. As part of the investigation, SEC staff collected communications from the personal devices of a sampling of various firm personnel, including senior executives. The SEC found that the use of "off-channel communications" at each of the firms was "pervasive" at all seniority levels, noting that it had found thousands or tens of thousands of off-channel messages about business matters at each of the firms. In the September 2022 announcement of charges against multiple firms, SEC Chair Gary Gensler explained the need to communicate "about business matters within only official channels," and he promised that the SEC would "continue to ensure compliance with these laws" in its investigations and enforcement work. Indeed, in early November, Gensler announced that the agency was continuing to investigate the use of platforms such as WhatsApp by firms subject to SEC oversight. And in their latest quarterly filings, at least three private equity firms disclosed that they had received inquiries from the SEC about their employees' use of third-party text

messaging applications.

The government's focus on this area extends far beyond these high-profile matters. Indeed, it has become routine in any investigation for the government to insist that companies forensically image their employees' personal devices, and that any document collection and production include data from third-party messaging apps. Claims that employees do not text or message about work will be met with skepticism; the government knows how common it is for employees to use these channels. Yet when a company seeks to comply with such a request from the government, it can expect serious resistance from its employees, who understandably seek to shield their personal data from scrutiny.

In navigating these competing interests, companies should also be mindful of local, state, federal and foreign privacy and labor laws that apply to employee data. For example, some laws grant employees rights over their data, including deletion rights, which could impair a company's ability to archive or share certain employee data. Similarly, companies that monitor the communications of their employees, including through mobile device management software, should ensure that they comply with applicable laws such as those on surveillance. Companies should keep in mind that laws governing employee data may apply irrespective of any DOJ, SEC, or other regulatory investigations or enforcement actions.

What can companies do now to address these issues?

- Implement or strengthen policies and procedures governing the use of personal devices and third-party messaging platforms.
    - Limit work-related communications to specific platforms and apps with settings prohibiting the permanent deletion of data – i.e., no work-related communications on "ephemeral and encrypted messaging applications" such as WhatsApp, Signal, etc.
    - Notify employees that data on their personal devices can and will be preserved, collected and produced if the devices are used for business purposes.
    - Conduct ongoing assessments to ensure that data on personal devices is preserved and can be collected if needed.
    - Include and enforce clear consequences for violating policies and procedures.
- Provide training on policies and procedures. It is not enough that the policies and procedures exist; companies must be able to demonstrate awareness, compliance and enforcement.
- Survey employees to understand use of personal devices and third-party messaging apps for work purposes. Survey responses will help companies better tailor their policies and procedures, as well as any related training.
- Consider the impact of privacy and labor laws that may apply to employee data and the company's related activities.

In addition, Monaco instructed the DOJ's Criminal Division to investigate and include corporate best practices on the use of personal devices and messaging apps in the next edition of its Evaluation of Corporate Compliance Programs, so be on the lookout for this publication, and update any policies and procedures as needed.

Contributors

Christian Lee
Bio

Alexandra Rex Mayhugh
Bio
