WhatsApp Messages May Be Gone But Never Forgotten – At Least Not By the DOJ: Your Company's 6-Step Action Plan

Insights
1.20.23

When your employees go "off-grid" and use unauthorized third-party messaging applications that fall beyond typical email and texting – like the self-destructing WhatsApp messages – they put you at increasing risk of scrutiny by federal criminal prosecutors, among other dangers. The inability to preserve such communications can cause regulatory record-retention headaches, interfere with your ability to respond to litigation discovery requests, put you at risk of violating consumer and employee privacy laws, and expose your sensitive or competitive business information. Not surprisingly, this problem has now found its way into the crosshairs of the Department of Justice (DOJ) given the resulting interference with the agency's ability to monitor employee misconduct and conduct criminal investigations of suspected corporate wrongdoing. What do you need to know about this modern trend – and what are the six steps you should consider implementing?

WhatsApp, Telegram, Signal, and the Modern Messaging Mess

In today's electronic era, most companies have a suite of authorized message applications and collaboration tools available to meet their employees' needs to conduct business. In addition, many companies now have policies related to employees' use of personal devices and authorized applications for work-related activities and communications.

However, your employees may also be using unauthorized messaging platforms to conduct business, ones beyond those typically provided and monitored by your company. Some of these have troublesome end-to-end encryption features and allow for ephemeral messaging (self-destructing messages). Examples include WhatsApp, Telegram, and Signal.

WhatsApp, for example, is the most-used instant messaging application in the world. It currently has over two billion global users (one quarter of the Earth's population) and handles over 100 billion message exchanges per day. In other words, the odds are good that your employees are using WhatsApp or a similar platform – the question becomes whether they are using them for business. If so, your company faces potentially enhanced criminal penalties when faced with a DOJ investigation.

The Monaco Memo Sends a Shot Across Your Digital Bow

Deputy Attorney General Lisa Monaco recently issued a memo (the "Monaco Memo") providing guidance to federal prosecutors when evaluating corporate cooperation and compliance programs in connection with their criminal investigations. This guidance outlines factors DOJ prosecutors should use when determining whether cooperating companies should be granted "cooperation credit" during an investigation.

Specifically, the 2022 Monaco Memo advises prosecutors "to consider whether the corporation has implemented effective policies and procedures governing the use of personal devices and third-party messaging platforms to ensure that business-related electronic data and communications are preserved." Cooperation credit can affect the form of the resolution, lessen the applicable fine range, and reduce possible jail time for individuals.

The Monaco Memo makes clear that a "robust compliance program" will have three components:

- effective policies about using personal devices and third-party messaging applications for work;
- employee training on these policies; and
- enforcement of policy violations.

In addition, the Monaco Memo advises prosecutors to consider whether a company seeking cooperation credit has implemented policies that allows it to provide the government with "all non-privileged responsive documents relevant to the investigation, including work-related communications . . . and data contained on phones, tablets, or other devices that are used by its employees for business purposes." This includes data located within the United States and abroad.

Businesses Left Adrift to Figure Out Next Steps – But We've Got Your Back

Unfortunately, the DOJ doesn't provide any specific examples of how a company can meet these requirements. Indeed, the Memo instructs the Criminal Division to study corporate best practices and to publish their results in the next edition of its Evaluation of Corporate Compliance Programs (these typically come out every few years). But the Criminal Division last updated this publication in June 2020.

But there's good news. While we wait for the Criminal Division to issue its update, we've been able to uncover a developing roadmap about how you should proceed. By reviewing recent settlements between a number of financial institutions and the Securities and Exchange Commission and the Commodity Futures Trading Commission, we can glean the best practices that put companies on the best footing.

These settlements arose from corporate failure to preserve and supervise employee business communications on personal devices and third-party messaging applications (specifically text and chat messages). From these settlements and guidance in the Monaco Memo, we've developed a six-

step action plan – including review and enhancement of corporate policies, employee training, technology solutions, monitoring, and enforcement action.

Your 6-Step Action Plan

Here are our suggested practical steps you should consider to shore up this risk-prone area in corporate communications:

1. **Audit Current Authorized Applications**: Review current corporate authorized business communication and collaboration platforms and devices to ensure appropriate record-retention capabilities. Where deficiencies exist, take remedial measures.
2. **Research Technology Solutions:** Identify easy-to-use collaboration and communication platforms to discourage use of unauthorized platforms for work. Authorized tools must have robust retention capabilities.
3. **Implement Policies**: Implement clear policies prohibiting use of personal devices and messaging and collaboration platforms unless company data and communications can be adequately preserved. Corporate policies should provide for review of personal devices by the company upon request.
4. **Comply with Record-Keeping Obligations:** Understand and comply with all laws mandating retention of certain records under federal and state statutory or regulatory schemes – such as the SEC's record-keeping requirements for broker-dealers, and state privacy laws such as the California Privacy Rights Act.
5. **Train Employees**: Implement employee training regarding the risks associated with use of personal devices and unauthorized applications for work and company policies concerning that use. This training should include a self-attestation of compliance.
6. **Monitor and Enforce Employee Compliance**: Monitor employee compliance with corporate policies, making employees' personal devices subject to review to assess compliance. Monitoring should include tracking usage by employees. Enforce violations with appropriate discipline, regardless of the employee's status within the company.

Conclusion

If you have questions regarding best practices for managing retention requirements for your electronic business records, please reach out to your Fisher Phillips attorney, the authors of this Insight, or any attorney in our eDiscovery and Digital Workplace Practice Group. Make sure you are subscribed to Fisher Phillips' Insight system to get the most up-to-date information on this and other employment topics directly to your inbox.

Related People

Wendy Hughes
Partner
610.230.6104
Email

Raymond W. Perez
Of Counsel
Email

Service Focus

Counseling and Advice

eDiscovery and Digital Workplace