DOJ guidance on ephemeral and third-party messaging apps: how to establish governance and drive compliance

Forensic & Integrity Services

January 2024

EY
Building a better working world

In the first of this three-part series, the EY Forensic & Integrity Services Team explores the steps to take now, next and beyond to effectively address Department of Justice (DOJ) guidance regarding ephemeral and third-party messaging apps while laying the foundation for a broader information governance program.

Regulators are taking action after years of debate about the use of ephemeral and third-party messaging apps.

Navigating the risks created by ephemeral and third-party messaging apps in the workplace is top of mind for companies considering the heightened regulatory activity over the past year. The Securities and Exchange Commission (SEC)1 and Commodity Futures Trading Commission (CFTC)2 issued fines totaling over $2.5B in 2022 and 2023 to companies for violations of record-keeping requirements stemming from use of third-party messaging applications. Regulatory scrutiny of these apps and the use of personal messaging to conduct business does not appear to be slowing down with the SEC's expansion of its ongoing "WhatsApp sweeps"3 and the release of its 2023 examination priorities, which continue to emphasize the importance of record-keeping for electronic communications.4 The DOJ Criminal Division's updated Evaluation of Corporate Compliance Programs (ECCP) guidelines, March 2023, marks an expansion of regulatory interest in ephemeral and third party messaging apps beyond financial services, and includes long-awaited guidance on how a compliance program's governance of employee use of personal devices and third-party messaging platforms and apps will be evaluated.

The DOJ put forth a series of questions aimed to guide prosecutors in their evaluation of a company's guidance and controls. What is clear from the inquiries outlined in the ECCP is that implementing effective governance over this complicated ecosystem of devices, platforms and apps requires engaging stakeholders from across the organization, including compliance, risk management, legal/litigation, IT, information security, records and information management, privacy and more. The multifaceted nature of this issue should be a "lightbulb moment" for companies to rethink ad hoc and siloed approaches to manage and control their information moving forward.

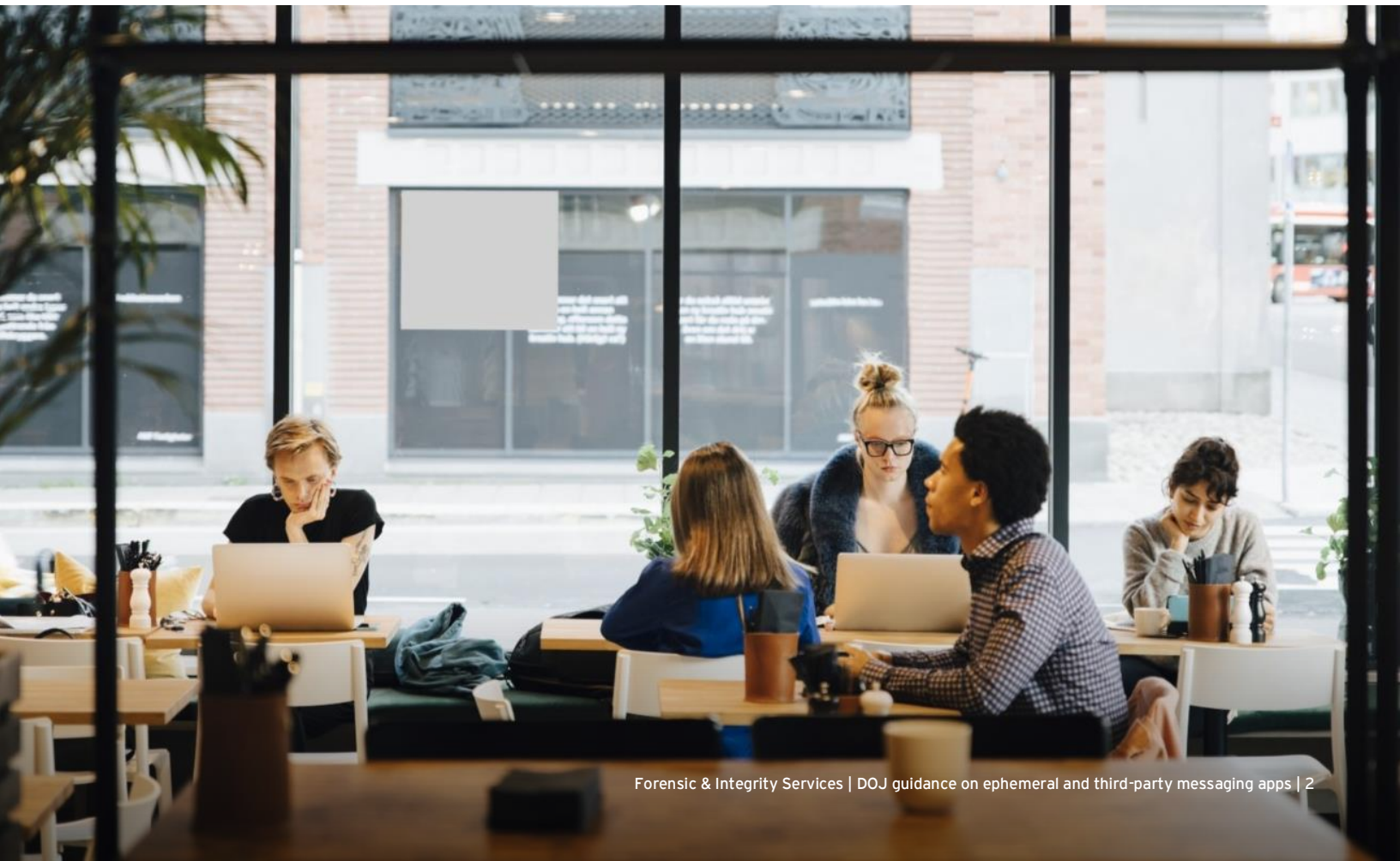
[1] https://www.sec.gov/news/press-release/2022-174
[2] https://www.cftc.gov/PressRoom/PressReleases/8599-22
[3] https://www.reuters.com/article/usa-sec-devices-idTRNIKBN2R61FP
[4] https://www.sec.gov/files/2023-exam-priorities.pdf

As regulatory guidance and scrutiny on ephemeral and third-party messaging apps continues to evolve, companies are realizing that data and technology are no longer just an "IT" issue.

Bring your own device (BYOD) programs and increasingly common remote/hybrid workplaces have introduced more than just "IT" risks. Compliance risks associated with data and technology also need to be identified, measured and mitigated. Many companies are starting to implement information governance programs to address the management of information risks that span domains, such as records and information management, legal processes, information security, data privacy and data governance. Bringing together the collective knowledge and expertise of these varied stakeholders enables companies to stay nimble and rapidly respond to changes in the evolving technology and data landscape in which they operate.

The diverse challenges posed by personal devices and third-party messaging applications illustrate the benefits of an information governance program. Information governance stakeholders can bring various perspectives and insights to the table, including:

- **Records and information management:** distinguishing business records and communications that need to be retained (and for how long) from nonbusiness records that can be purged or deleted
- **Legal/litigation:** determining approaches and considerations for complying with obligations to preserve information for regulatory or legal matters
- **Privacy:** balancing company surveillance activities with evolving data privacy obligations
- **Business:** determining business needs and related emerging technologies to enable the company to remain competitive
- **Information technology:** identifying the technical capabilities of various platforms to support preservation, retention, deletion, and limitations or consideration for enabling different settings
- **Information security:** understanding the potential for data loss and misuse for different technologies
- **Compliance:** considering the relevant laws and regulations when implementing policies and how policies will be enforced



Steps to take Now, Next and Beyond

Ephemeral and third-party messaging apps pose unique challenges for companies, and traditional ways of identifying, managing and governing this technology may not be as effective due to the emerging nature of these risks, issues and the technology itself.

Now: Support proactive initiatives designed to drive compliance and reduce risk:

- Assess current employee use of personal devices and third-party applications to identify potential risk areas or compliance violations.
- Review, align and update policies and procedures (e.g., acceptable use, BYOD, records and information management, legal hold and preservation).
- Evaluate technology to support compliance (e.g., enhanced functionality or tools that enable capture, retention and archival capabilities).
- Train employees on information risks and new requirements and promote a culture of compliance.
- Consider enterprise licenses for key communication and collaboration platforms that offer elevated control and compliance functionality.
- Adapt a more agile mobile device management (MDM) program to address variable risks in employee populations.

Next: Prepare for reactive regulatory inquiries and investigations to enable timely and complete responses to regulators and courts:

- Develop legal hold processes and train employees and IT system owners to enable timely preservation.
- Leverage technology to issue, track, monitor and lift legal holds.
- Identify and define key data sources that have frequently been subject to legal hold and collection.
- Understand retention and disposition practices, including preservation and collection considerations.
- Define forensic collection standards, processes and technologies, including appropriate data transfer and chain of custody protocols.
- Evaluate forensic acquisition tools and techniques needed to collect information from nonstandard data sources.

Beyond: Establish an information governance program to manage information risks in an evolving business, technology and regulatory environment:

- Socialize the value of a holistic information governance program across the organization to support an enhanced understanding of information risk and the benefits to mitigate fines and reputational risks associated with regulatory enforcement or other public incidents.
- Establish a cross-functional governance structure and operating model.
- Harmonize policies, standards and procedures across information risk domains to drive consistency in terminology and requirements.
- Centralize information risk monitoring activities through standardized methodologies and reporting structures.

EY Forensic & Integrity Services Team

The EY Forensic & Integrity Services team brings together our digital forensics experience to collect ephemeral and third-party messaging data with our experience working with companies to effectively manage complex information risks to support an integrated approach that addresses the emerging technology challenges and evolving regulatory compliance requirements.

Our professionals bring extensive skills and experience serving corporate legal and compliance departments and have served as fact and expert witnesses in regulatory matters and litigation. We frequently publish thought leadership related to the intersection of records and information management, data privacy and legal preservation, and other information risk domains, particularly as they pertain to emerging technology, evolving regulations and their impact on information governance programs. Our team of professionals also includes former prosecutors from the Department of Justice, former investigators from the Federal Bureau of Investigation and former regulators from the United States Securities & Exchange Commission.

We serve as trusted advisors to our clients, bringing our approaches and recommendations to complex global issues impacting companies today. We understand regulators' viewpoints and are intimately familiar with the challenges that companies face when developing policies and procedures to support an effective information governance program. Our combination of experienced investigators and information governance consultants yields unique insights into what will matter when these emerging information and technology risks come to fruition.

Read more at www.ey.com/us/forensics.

Contact us – Ernst & Young LLP

Jennifer Joyce
Principal, EY Americas
Forensic & Integrity Services
Information Governance Leader
+1 703 747 0620
jennifer.joyce@ey.com

Kymberli Shoemaker
Senior Manager, EY Americas
Forensic & Integrity Services
Information Governance
+1 703 747 0318
kymberli.shoemaker@ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

2410-10433-CS | ED None

ey.com/us/forensics/discovery