Morgan Lewis

RILA COMPLIANCE COUNCIL EPHEMERAL MESSAGING

April 13, 2023

Presenters

Amy E. Schuh

Scott Milner

Morgan Lewis

Changes to the Corporate Compliance Program Evaluation Criteria (March 2023)

On March 3, 2023, the Criminal Division released an updated version of its Evaluation of Corporate Compliance Programs (ECCP) guidance—the first update since June 2020.

- Key additions include:
  - Significant additions around what companies are doing to understand the communication channels employees use and ensure retention of that data. Specific focus on the use of third party messaging applications and how the company manages the risk and retention of this means of communication.
  - Significant additions to the previous "Incentives and Disciplinary Measures" section, retitled "Compensation Structures and Consequence Management"; including simultaneous announcement of the release of the Compensation Clawback Pilot Program, the revised ECCP directs prosecutors to examine a company's compensation systems and whether those incentivize complaint conduct or not—for example, by clawing back compensation for those found to be involved in misconduct or tying compliance as a metric into bonuses to reward good compliance.

Paramount Concern…

the requirement that they give the company access to these communications? Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization's compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies? How does the organization manage security and

DOJ will be focusing on this issue, and failure to demonstrate an ability to retain, collect and produce business records relevant to an investigation may result in a finding that the company does not have an effective compliance program

Policies & Processes

- What electronic communication channels are used by employees? What channels does the company allow its employees to use? How does that practice vary by jurisdiction and business function, and why?
- Does the company have policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging applications? Are they tailored to the corporation's risk profile and specific business needs?
- Is the organization's approach to permitting and managing communication channels, including BYOD and messaging applications, reasonable in the context of the company's business needs and risk profile?
- What is the rationale for the company's approach to determining which communication channels and settings are permitted?
- How does the company communicate these policies and procedures to employees?

SUMMARY

Controls, Monitoring & Enforcement

- What specific policies and processes have you implemented to enable you to retain, collect and produce communications?
- What efforts are you employing to monitor compliance with these policies and processes?
- What actions have you taken if you discover a violation of any policy or process?

DETAILS

What mechanisms has the company put in place to manage and preserve information contained within each of the electronic communication channels?

What preservation or deletion settings are available to each employee under each communication channel, and what do the company's policies require with respect to each?

If the company has a policy regarding whether employees should transfer messages, data, and information from private phones or messaging applications onto company record-keeping systems in order to preserve and retain them, is it being followed in practice, and how is it enforced?

What policies and procedures are in place to ensure that communications and other data is preserved from devices that are replaced?

Has the company enforced these policies and procedures on a regular and consistent basis?

What are the consequences for employees who refuse the company access to company communications?

Has the company ever exercised these rights?

Has the company disciplined employees who fail to comply with the policy or the requirement that they give the company access to these communications?

Things to Consider

Information Governance (IG)	• Policy Updates to Address Potential Use of Ephemeral Messaging
	  • Reflect actual practice
	  • Include reminders of appropriate and inappropriate use of ephemeral messaging
	  • What to do when ephemeral messaging requires retention

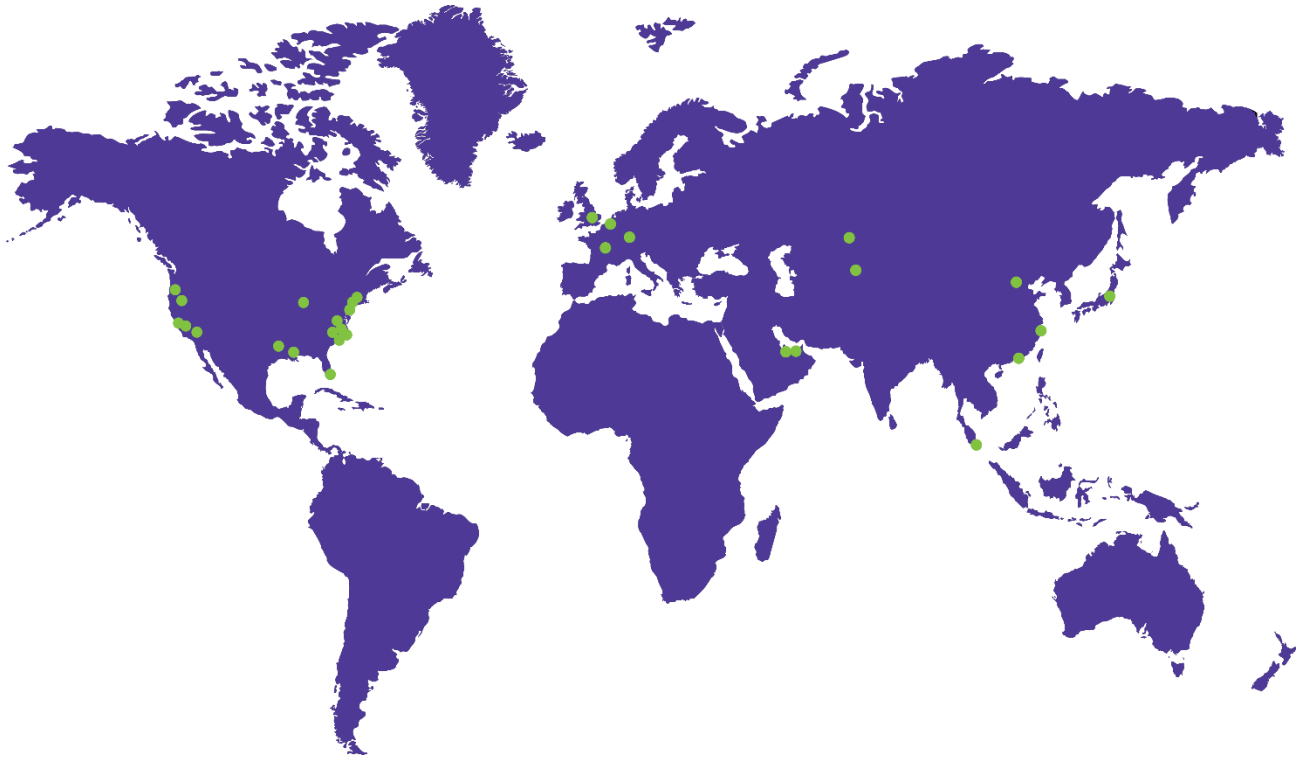
Preservation	• Update legal hold templates to identify ephemeral messaging is ESI and appropriate ongoing use or lack of use of ephemeral messaging apps • Create FAQ to address common questions including how to preserve • Develop playbook for how you are going to preserve and collect
Collection, Processing & Analysis	• Develop playbook for collection options • Develop defaults for data processing and review
Monitoring	• Consider timing and how to monitor since ephemeral messaging does not automatically "synch" to company network • Use of existing or new tools to help determine when employees are using "shadow" IT tools to trigger follow-up

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Abu Dhabi
Almaty
Beijing*
Boston
Brussels
Century City
Chicago
Dallas
Dubai
Frankfurt
Hartford
Hong Kong*
Houston
London
Los Angeles
Miami
New York
Nur-Sultan
Orange County
Paris
Philadelphia
Pittsburgh
Princeton
San Francisco
Shanghai*
Silicon Valley
Singapore*
Tokyo
Washington, DC
Wilmington



Morgan Lewis

THANK YOU