The Government Expects Me to Do What?! Managing Business Data in the Era of Messaging Apps, Remote Work, and BYOD

Guest and Dorsey Panelists

Nancy Hendrickson, Vice President and Associate General Counsel, D.A. Davidson Companies

Elizabeth Moellering, Senior Associate General Counsel, Optum

Nicole Engisch and **Caroline Sweeney**, Dorsey & Whitney LLP

Program Materials

PowerPoint Presentation

Dorsey Publications

Dorsey eUpdate: *Department of Justice Seeks to Reward Due Diligence and Timely Self-Disclosures in Mergers & Acquisitions Through New Safe Harbor Policy*, Nicole Engisch, Jaime Stilson & RJ Zayed (October 16, 2023)
https://www.dorsey.com/newsresources/publications/client-alerts/2023/10/doj-safe-harbor-policy

Dorsey eUpdate: Department of Justice Announces First-Ever Pilot Program on Compensation Incentives and Clawbacks, Revisions to Corporate Guidance Regarding Electronic Communications, and Resource Commitments for Corporate Compliance with Sanctions and Export Control Laws, Nicole Engisch, John Marti & Elena Modl (March 6, 2023)
https://www.dorsey.com/newsresources/publications/client-alerts/2023/3/doj-announces-program-on-compensation-incentives

Dorsey eUpdate: DOJ Announces Additional Incentives for Corporate Cooperation in Criminal Enforcement, RJ Zayed, Katherine Chaves & Elena Modl (January 26, 2023)
https://www.dorsey.com/newsresources/publications/client-alerts/2023/1/doj-incentives-for-cooperation

Session materials are available for download on www.dorsey.com.
Search: "Corporate Counsel Symposium 2023"

The Government Expects Me to Do What?! Managing Business Data in the Era of Messaging Apps, Remote Work, and BYOD

Nancy Hendrickson, D.A. Davidson Companies
Elizabeth Moellering, Optum
Nicole Engisch and Caroline Sweeney, Dorsey & Whitney LLP

November 14, 2023

Housekeeping

In Person Attendees

Materials are available on Dorsey.com or scan the QR Code.
Attendance Sheets are on the tables. Remember to sign-in for each session.

Webinar Attendees

Materials are available in the Zoom Events Lobby or scan the QR Code.
The Attendance Sheet is available for download from the Zoom Events Lobby. Return to attendance@dorsey.com.
A CLE Code will be announced for states that require a Code.

The speakers will not have time for questions. Please contact the speakers or your trusted Dorsey contact.

Scan for Materials

CCS corporate counsel symposium

DORSEY always ahead

Guest and Dorsey Speakers

Nancy Hendrickson
Vice President & Associate General Counsel
D.A. Davidson Companies

Elizabeth Moellering
Senior Associate General Counsel
Optum

Nicole Engisch
Partner
Dorsey & Whitney LLP

Caroline Sweeney
Director, Knowledge Management/Innovation
Dorsey & Whitney LLP

CCS corporate counsel symposium

DORSEY always ahead

Agenda

- What are the issues?
  - What is ephemeral messaging and related messaging?
- Benefits of messaging apps and personal devices
- Challenges to preserving and collecting
- Why does this matter?
- What does DOJ expect?
- What does SEC expect?
- What do civil litigants and courts expect?
- So what should you do?
  - Weigh benefits/assess risks
  - Recommended solutions
  - Suggested policy provisions
  - Final takeaway points

CCS corporate counsel symposium

DORSEY always ahead

Types of Messaging

- **Snapchat, Telegram, Hash, Cover Me, Confide, Wickr, Wire**
  - **Ephemeral: deliberately and automatically delete messages (and metadata) by default for both sender and recipient, and no archiving**
- **WhatsApp, Instagram, WeChat, Facebook Messenger, Signal, Slack**
  - **Quasi-ephemeral: may be set to preserve or delete, and metadata is preserved**
- **iMessage, SMS texts**
  - **Non-ephemeral: sender cannot automate deletion for both sender and recipient—recipient has to manually delete (and even deleted texts may still be recoverable)**

CCS corporate counsel symposium

DORSEY always ahead

What Are the Issues?

- **Pandemic increased remote work and increased use of personal devices (BYOD policies) and ephemeral messaging for business**
- **Government (and civil litigants) are focused on these data sources**
- **But these data sources create huge challenges for preservation and collection**

CCS corporate counsel symposium

DORSEY always ahead

Benefits of Messaging Apps and Personal Devices

- More and more employees prefer texts/chats over email
- Messaging Apps are convenient and relatively secure
  - Don't need IT infrastructure
  - Encrypted end-to-end with effective authentication
- Messaging Apps may comply with data privacy and data protection laws (esp. cross border)
- Less data on company servers may lessen data breach exposure
- Perceived increase in efficiency and cost savings

CCS corporate counsel symposium

DORSEY always ahead

Challenges for Preservation/Collection (Messaging Apps)

- By their nature, ephemeral messaging apps automatically delete data
- Companies' IT depts. can't just implement holds behind the scenes like they can with email
- Traditional forensic imaging doesn't work with ephemeral messaging apps
- Companies may not know which messaging apps employees are using

Challenges for Preservation/Collection (Personal Devices)

- Companies don't have actual possession of devices
- Employees may resist giving up their phones or passwords
- Employees may expect more privacy (and may invoke bargaining agreements and legal protections)
- Phone imaging is expensive, time-consuming, and the data may not be easily reviewed
- Employees may not acknowledge they have business data
  - Do they understand what a "business communication" is?
- Devices can be lost, stolen, or damaged (or claimed to be)

Challenges for Preservation/Collection (Personal Devices Cont'd)

- Users (and settings) may delete data over time
- Employee may not be sole owner of device (limiting access to data)
- Data may be stored separately from device
- Mobile device management software currently can track usage and can selectively delete data, but doesn't yet collect most data
- Even if a company requires employees to have a separate phone, employees may still use personal devices for business purposes anyway

Why Does This Matter?

- DOJ and SEC (and CFTC) are focused on preservation of ephemeral messaging and bus. data on personal devices
  - Concerned about hidden evidence of crimes
- SEC's policies have the force of law, and SEC has imposed significant financial penalties
- DOJ's policies lack the force of law, but can impact how DOJ makes charging/settlement decisions
- Civil litigants and courts also want this data preserved and collected
- Foreign regulators (EU, UK, Hong Kong, etc.) are also focusing on ephemeral messaging

DOJ Expects Companies to Preserve the Data

- In 2017, DOJ incentivized companies *to prohibit* use of ephemeral messaging
- Since 2019, DOJ incentivizes companies *to preserve* the business info.
- Fits with DOJ's overall corporate enforcement and voluntary self-disclosure policies:
  - Companies should timely preserve/collect/produce all relevant, non-privileged information to get cooperation credit

DOJ Expects Companies to Preserve the Data

- **AAG Kenneth Polite Speech 3/3/23 at the ABA's National Institute on White Collar Crime**
  - **If company under investigation has not produced data from messaging applications, "prosecutors will not accept that at face value"**
  - **Prosecutors will "ask about the company's ability to access such communications."**
  - **"A company's answers – or lack of answers – may very well affect the offer it receives to resolve criminal liability."**
  - **"So when crisis hits, let this be top of mind."**

DOJ Expects Companies to Have Effective Policies

- **Company policies regarding use of personal devices and messaging apps should:**
  - **Be tailored to the company's risk profile and specific business needs**
  - **Ensure to the greatest extent possible that business communications are preserved and accessible to the company**
  - **Be communicated to employees and regularly and consistently enforced**
  - **Be well-designed, applied earnestly and in good faith, and work in practice**

See Evaluation of Corp. Compliance Programs Policy (2023)

DOJ Expects Companies to Have Effective Policies

- **Company's policies should address:**
  - **Communication Channels: which channels are used for business data and why; what mechanisms are in place to preserve data (deletion settings, etc.)**
  - **Policy Environment: what policies ensure company can access and preserve business data on personal devices and messaging apps**
  - **Risk Management: how does the company manage communications, including BYOD and mess. apps., given its risk profile; how does it regularly test/audit compliance, what are the consequences for employees who violate policies**

DOJ's Similar Expectations for Civil Cases

- **DOJ may consider the nature and effectiveness of a compliance program when evaluating a resolution in civil False Claims Act matters**
  - **DOJ will evaluate compliance programs using the same criteria applied by the criminal division (includ. for BYOD/mess. apps)**

See Justice Manual 4-4.112 – Guidelines for Taking Disclosure, Cooperation, and Remediation into Account in False Claims Act Matters

CCS corporate counsel symposium

DORSEY always ahead

CLE Code
for
Webinar Attendees Only

Tip: The CLE code is for States that Require a Code, like New York.
Tip: The CLE code is different than the event code assigned by states.

CCS corporate counsel symposium

DORSEY always ahead

SEC Recommends Companies Prohibit Ephemeral Messaging Apps

- **In 2018, SEC's National Office of Compliance Inspections and Examinations advises regulated entities to:**
  - **Prohibit "business use of apps . . . that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third party viewing or back-up."**

SEC Requires Companies to Preserve the Data

- ***Broker-dealers*** **must preserve originals of all communications to/from the broker-dealer that relate to its business for at least three years**
  - **Rule 17a-4 of the Securities Exchange Act of 1934 (17 CFR § 240.17a-4)**
- ***Registered investment advisers*** **must preserve originals of all communications relating to recommendations or advice and certain client-specific transactional communications for at least five years**
  - **Rule 204-2(a)(7) of the Investment Advisers Act of 1940 (17 CFR §§ 275.204-2(a)(7) and (e)(1))**
- ***Both broker-dealers and registered investment advisers*** **must supervise employees to ensure compliance with recordkeeping obligations**
  - **Release No. 2022-174, U.S. Sec. & Exch. Comm'n, "SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures," Sept. 27, 2022.**

SEC Requires Companies to Preserve the Data

- ***Public company issuers***: **While there's no precise rule, under Sec. Exchange Act Section 13(b)(2)(A), public company issuers are required to make and keep certain books and records that accurately and fairly reflect the transactions and dispositions of the assets of the issuer**
- ***Swap dealers***: **The Commodity Exchange Act, Section 4s(f)(1)(C) (7 U.S.C. 6s(f)(1)(C)) requires registrants to "keep books and records of all activities related to its business as a swap dealer"**
- **Duty to preserve data is likely triggered whenever litigation is reasonably anticipated or foreseeable**
  - ***See*** **SEC's Enforcement Manual**

Recent Major SEC Enforcement Actions

- **September 2022: 15 broker-dealers and one affiliated investment adviser failed to maintain ephemeral messages that fell within Rule 17a-4 and Rule 204-2. Combined penalties exceeded $1.8 billion**
- **August 2023: 9 broker-dealers and one dually registered broker-dealer and investment adviser engaged in widespread and longstanding failures to preserve electronic communications through messaging apps on personal devices. Combined penalties exceeded $289 million**
- **September 2023: five broker-dealers, three dually registered broker-dealers and investment advisers, and two investment advisers engaged in widespread and longstanding failures to preserve electronic communications personal texts and off-channel communications regarding advice and recommendations. Combined penalties exceeded $79 million**

What Do Civil Litigants and Courts Expect?

- **Party shall produce relevant electronically stored information (ESI) in the party's possession, custody, or control. ***
- **Three main issues re. whether ESI is subject to discovery:**
  1. **Does the company have poss., custody, or control over the ESI?**
  2. **Is the ESI relevant and unique or duplicative of other data from other sources?**
  3. **Is discovery of the ESI "proportional?"**
- **Failure to take reasonable steps to preserve texts and messages, as with email and other ESI, may constitute spoliation and may result in sanctions under Rule 37(e)**

***Fed. R. Civ. P. 26(a); 34(a); 45(a)**

What Do Civil Litigants and Courts Expect?

- **Courts interpret "possession, custody or control" differently**
  - **"legal right" theory: Does the party have a legal right to access the data?**
  - **"practical ability" theory: Does the party have a legal right or the actual capability to obtain the data?**
- **Rule 26(a) proportionality factors**
  - **issues at stake, amount in controversy, parties' relative access to relevant information, parties' resources, importance of the discovery in resolving the issues, and balancing expense of the discovery against likely benefit**
  - **Privacy considerations?**

Poss., Custody or Control Over Phones

- ***Cotton v. Costco Wholesale Corp.*, 2013 WL 3819974 (D. Kan. July 24, 2013) (denying motion to compel because "Costco does not likely have within its possession, custody, or control text messages sent or received by these individuals on their personal cell phones").**
- ***Alter v. Rocky Point Sch. Dist.*, No. 13 Civ. 1100, 2014 WL 4966119, at *10 (E.D.N.Y. Sept. 30, 2014) ("to the extent that the School District employees had documents related to this matter, the information should have been preserved on whatever devices contained the information (e.g. laptops, cellphones, and any personal digital devices capable of ESI storage)")**
- ***Lalumiere v. Willow Springs Care, Inc.*, 2017 WL 6943148 (E.D. Wash. Sept. 18, 2017) (employer "does not possess or control the text messages from the personal phones of its employees and may not be compelled to disclose text messages from employees' personal phones")**

Poss., Custody or Control Over Phones

- ***Halabu Holdings v. Old Nat'l Bancorp***, **2020 WL 12676263 (E.D. MI, June 9, 2020) (in the absence of a BYOD agreement that defines rights and responsibilities regarding personal cell phone use in connection with employer's business, employer does not have poss., custody or control over personal cell phone)**
- ***Krishnan v. Cambia Health Solutions, Inc.*, 2021 WL 3129940 (W. D. Wash. 2021) (defendant did not have poss., custody, or control over employees' personal phones and not compelled to produce texts, but employer might have poss., custody, or control of a cell phone when the employer issued the phone, the phone is used for business purposes, and the employer has a legal right to obtain communications from the cell phone)**
- ***In re Pork Antitrust Litig.*, 2022 WL 972401 (D. Minn. March 31, 2022) (no poss., custody, or control over employees' personal phones because no access to text messages and BYOD policy defined company information as "all data that is sourced from company systems and synced between the mobile device and its servers")**

Duty to Preserve

- **Once duty to preserve attaches, parties need to preserve relevant info.**
- **Duty to preserve is triggered:**
  - **When served with subpoena or other demand**
  - **When litigation is reasonably anticipated, foreseeable or when pending**
  - **"A variety of events may alert a party to the prospect of litigation." Fed. R .Civ. P. 37(e), advisory committee's note to 2015 amendment.**

Sanctions For Failure to Preserve

- ***Paisley Park Enters., Inc. v. George Ian Boxill, Rogue Music Alliance, LLC***, **330 F.R.D. 226 (D. Minn. 2019) (court sanctioned defendants for failure to suspend the auto-delete function on personal phones, failure to put in place a litigation hold to ensure preservation of text messages, failure to determine if they could recover the missing text messages by use of the "cloud" function or through consultation with a software expert).**

- ***Herzig v. Arkansas Foundation for Medical Care Inc.*, 2019 U.S. Dist. LEXIS 111296 (W.D. of Ark. 2019) (court dismissed plaintiffs' case because they used ephemeral messaging application Signal, intentionally destroying evidence that was subject to legal holds)**

Sanctions For Failure to Preserve

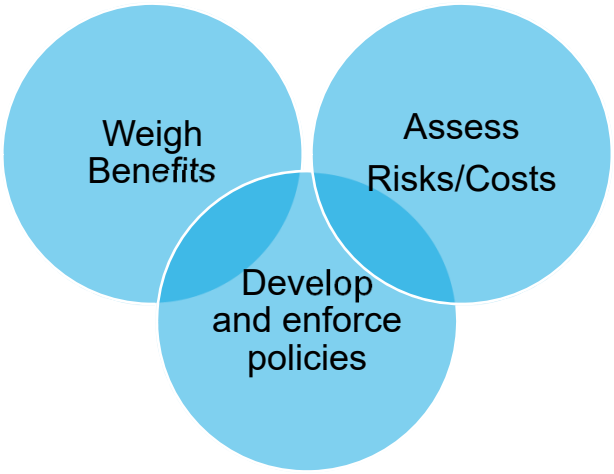
- ***Federal Trade Commission v. Noland*, 2021 WL 3857413 (D. Ariz. Aug. 30, 2021) (court entered adverse inference that spoliated evidence was unfavorable to defendants; the day after company learned of FTC inquiry, officers began using ephemeral messaging apps and auto deleted all messages, despite FTC's directive to preserve documents document destruction)**

- ***In re Google Play Store Antitrust Litig. Litig.*, 2023 WL 2673109 (N.D. Cal. Mar. 28, 2023) (court sanctioned Google because after litigation hold, Google failed to suspend automatic deletion of internal company chat messages and failed to adequately supervise the preservation efforts of employees)**

CCS corporate counsel symposium

DORSEY always ahead

So What Do You Do?



CCS corporate counsel symposium

DORSEY always ahead

Weigh the Benefits

- **What are your company's benefits from ephemeral messaging apps/BYOD policies?**
  - **How do they meet business objectives?**
  - **How widely do your employees use messaging apps/personal devices (consider polling them)?**
  - **Does your company benefit from these uses because of enhanced security, data minimization, compliance with international law, etc.?**
  - **Cost savings/efficiencies?**

CCS corporate counsel symposium

DORSEY always ahead

Assess Your Risks

- **What are your company's risks related to ephemeral messaging apps/BYOD policies?**
  - **How widely do employees use messaging apps/personal devices?**
  - **Are you in a highly regulated industry, esp. one subject to SEC regulation?**
  - **Have you had DOJ investigations before? Do you foresee the potential for involvement with DOJ?**
  - **Are you frequently involved in civil litigation?**
  - **Do you operate across international jurisdictions that are also regulating these data sources?**
  - **Do your jurisdiction's privacy laws and legal record retention requirements impact your ability to access and preserve any of this data?**
  - **What are your company's risks of data breach exposure?**

CCS corporate counsel symposium

DORSEY always ahead

Recommended Solutions-Before Duty to Preserve

- **Develop and implement effective policies regarding preservation and access to (collection of) business data when on personal devices and on messaging apps (esp. ephemeral messaging apps)**
- **Train employees on the policies**
- **Run "audits" to be sure policies are effective (e.g., random audits of personal devices to ensure policies are followed)**
- **Consider asking employees to affirm at least annually compliance with preservation and data retention requirements**
- **Discipline employees who fail to comply with policies**
- **Look for technology solutions**

Recommended Solutions-After Duty to Preserve

- Notify employees of litigation holds (and enforce)
- Suspend use of ephemeral messaging and adjust deletion settings
- Attempt to collect relevant data from all sources
- Interview custodians who may have used ephemeral messaging/personal devices
  - Verify responses
- Memorialize preservation and collection efforts
- Determine if costs to collect, review and produce are preferred over costs to move to quash (and risks of sanctions)

Suggested Policy Provisions

- Describe acceptable uses of personal devices and permitted apps for particular business activities (e.g., limited to scheduling calls)
  - Address popular apps in policy even if prohibited
- Explain/obtain consent to company's ownership/control over business data
- Describe what is required for preservation and deletion settings
- Establish proactive legal hold procedures before investigations or litigation
- Describe mobile device management (MDM) software to be installed
- Mandate policies/adopt software to disable or control data deletion in some circumstances (e.g., after duty to preserve)
- Explain security measures (multi-factor authentication, etc.) and requirements imposed on an employee's access to the network
- Integrate with other data use and retention policies
- Describe process for departing employees
- Provide notice that company will monitor/enforce policy to ensure compliance

Final Takeaway Points

- Don't ignore personal devices and messaging apps.
- Adopt policies appropriate to your risk profile (spell out what's OK and what's not OK) and then actively enforce those policies
- The goal is to either be in a position to collect and produce responsive business data on personal devices or messaging apps or reasonably explain why you can't

Thank you for attending!

Need Credit?

In-Person attendees remember to sign-in on the green sheets for each session.

Webinar Attendees return your completed sign-in to attendance@dorsey.com. Certificates will be sent to those who return the completed form.

Download Materials from Dorsey.com (search "Corporate Counsel Symposium 2023") or scan the QR code.

Legal Notice

This presentation is intended for general information purposes only and should not be construed as legal advice or legal opinions on any specific facts or circumstances. An attorney-client relationship is not created through this presentation.