wgs

The Sedona Conference

Commentary on Discovery of Mobile Device Data

A Project of The Sedona Conference Working Group
on Document Retention and Production (WG1)

May 2025
Public Comment Version
Submit comments by July 7, 2025,
to comments@sedonaconference.org

The Sedona Conference Commentary on Discovery of Mobile Device Data

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

MAY 2025 PUBLIC COMMENT VERSION

Drafting Team Leaders

Dennis Kiker Michelle Newcomer

Drafting Team

Alicia Clausen Shauna Itri
Rachel Kaufman Warren Kruse
Jason Lichter Maggie Malloy
John Pappas Robin Perkins
Lars Schou Deric Yoakley

Steering Committee Liaisons

Robert Keeling Daniel Lim
Kelly McNabb Maria Salacuse

Staff Editor: Craig Morgan

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the "Sponsors" navigation bar on the homepage of our website.

Preface

Welcome to the May 2025 Public Comment Version of The Sedona Conference's *Commentary on Discovery of Mobile Device Data*, a project of The Sedona Conference Working Group 1 on Electronic Document Retention and Production (WG1). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of complex litigation, cross-border data flow, intellectual property rights, data security and privacy, and the impacts of artificial intelligence.

The mission of The Sedona Conference is to move the law forward in a reasoned and just way. The mission of WG1, formed in 2002, is "to develop principles, guidance and best practice recommendations for information governance and electronic discovery in the context of litigation, dispute resolution and investigations." WG1 has published the authoritative *Sedona Principles* addressing electronic document production and several companion works, including guidelines for electronic document management, several commentaries on eDiscovery related topics, and cooperation guidance for trial lawyers, in-house counsel, and the judiciary.

The WG1 Brainstorming Group to develop this *Commentary* was launched in December 2022. The Group's report and recommendations were presented at the WG1 Midyear Meeting in Portland, Oregon in April 2023, with a Drafting Team formed in January 2024. The Team's report and recommendations were circulated to the WG1 membership and the subject of dialogue at the April 2024 Midyear Meeting in Arlington, Virginia. The final draft was submitted in January 2025. The editors have reviewed the comments received through the Working Group Series review and comment process.

This *Commentary* represents the collective efforts of many individual contributors. On behalf of The Sedona Conference, I thank in particular Drafting Team Leaders Dennis Kiker and Michelle Newcomer, and WG1 Steering Committee Liaisons Robert Keeling, Daniel Lim, and Maria Salacuse. I also thank the volunteer efforts of the entire Drafting Team: Alicia Clausen, Shauna Itri, Rachel Kaufman, Warren Kruse, Jason Lichter, Margaret Malloy, John Pappas, Robin Perkins, Lars Schou, Daniel Stromberg, and Deric Yoakley. The drafting process for this *Commentary* has also been supported by the entire WG12 Steering Committee.

Please note that this version of the *Commentary* is open for public comment through July 7, 2025, and suggestions for improvements are welcome. After the deadline for public comment has passed, the drafting team will review the public comments and determine what edits are appropriate for the final version. Please send comments to comments@sedonaconference.org.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of artificial intelligence and the law, electronic document management and discovery, cross-border discovery and data protection law, international data transfers, data security and privacy liability, and patent litigation best practices. The Sedona Conference hopes and anticipates that the

output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be.

Kenneth J. Withers
Executive Director
The Sedona Conference
May 2025

Table of Contents

I. INTRODUCTION

The use of mobile devices is ubiquitous. As a result, it is not surprising that they are an increasingly relevant data source in litigation. The unique nature of mobile device data raises complex issues that are not often raised or addressed in sufficient detail by the courts to provide parties and practitioners with a clear legal framework for meeting their discovery obligations related to mobile device data.

Accordingly, this *Commentary* provides both legal and practical guidance to parties, counsel, and the courts on relevant standards and factors impacting discovery of mobile device data, while addressing evolving technical issues affecting this type of data. To this end, it provides guidance for preserving, collecting, processing, searching, reviewing, and producing mobile device data. Each matter is unique, however, and nothing in this *Commentary* should be interpreted as endorsing any method for satisfying a party's discovery obligations with respect to mobile device data. Likewise, because mobile device technology changes rapidly, this *Commentary* provides guidance applicable to mobile device data generally, and not with respect to any particular make, model or mobile device operating system.

Finally, in keeping with the core principles underpinning The Sedona Conference, this *Commentary* encourages cooperation among parties and their counsel with respect to each stage of the discovery process.[1]

---

1 The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 125 (2018) [hereinafter *The Sedona Principles, Third Edition*] ("In addition to what is required by th[e] [Federal] Rules [of Civil Procedure], it is generally in the best interests of the responding party to engage in meaningful cooperation with opposing parties to attempt to reduce the costs and risk associated with the preservation and production of ESI.").

II. WHAT IS A MOBILE DEVICE AND WHAT DATA CAN BE STORED ON OR ACCESSED FROM A MOBILE DEVICE?

There is no single, universally accepted definition of "mobile device."[2] Many courts have resolved disputes concerning mobile device discovery,[3] but there are few, if any, published decisions expressly defining the term mobile device and what it does (and does not) encompass.

Perhaps in response to the lack of judicial guidance, some parties have elected to include their own definitions of a mobile device in electronically stored information (ESI) discovery protocols. For instance, in *Loomis Sayles Trust Co., LLC v. Citigroup Global Markets Inc.*, the court entered an ESI protocol in which the parties defined "Mobile Device" as "any mobile phone, cellular phone, or tablet device (e.g., iPhone, iPad, Android-compatible devices, or Microsoft Surface Go)."[4] Definitions of this sort, however, can be problematic in their reliance on specific make/model examples rather than universal criteria that can be applied to new types of devices.[5]

Accordingly, in defining a mobile device for purposes of this *Commentary*, we look to other leading industry resources. Most significantly, The National Institute of Standards and Technology (NIST)[6] has created a glossary of terms and definitions that are referenced in its cybersecurity and privacy standards, guidelines, and other technical publications, which includes no fewer than nine distinct

---

2 The Sedona Conference has not defined "mobile device." *The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition,* 21 SEDONA CONF. J. 263 (2020).

3 *See generally In re* Pork Antitrust Litig., No. 18-CV-1776 (JRT/HB), 2022 WL 972401 (D. Minn. Mar. 31, 2022); Miramontes v. Peraton, Inc., No. 3:21-CV-3019-B, 2023 WL 3855603 (N.D. Tex. June 6, 2023); Laub v. Horbaczewski, 331 F.R.D. 516, 527 (C.D. Cal. 2019).

4 Loomis Sayles Trust Co., LLC v. Citigroup Global Markets Inc., No. 1:22-cv-06706-LGS (S.D.N.Y. Jan. 24, 2023) ("*Loomis*").

5 While technically a device that is portable, the *Loomis* parties' characterization of Microsoft's Surface Go tablet as a mobile device is at odds with this Commentary's guidance that devices that run operating systems generally associated with desktop and laptop computers (here, Windows) should *not* be conflated with mobile devices that are the subject of this Commentary. Other Sedona guidance is more directly applicable to those devices that run Windows and Mac operating systems. *See The Sedona Principles, Third Edition*, *supra* note 1; The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 (2018) [*hereinafter Commentary on BYOD*].

6 The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S. Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Congress established the agency to remove a major challenge to U.S. industrial competitiveness at the time — a second-rate measurement infrastructure that lagged behind the capabilities of the United Kingdom, Germany and other economic rivals." *See* https://www.nist.gov/about-nist (last visited Jan. 6, 2025). NIST's mission is to "promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life". *Id.* As such, NIST develops standards, guidelines and best practices pertaining to technology and data security used by federal agencies and businesses.

mobile device definitions across its numerous publications.[7] This *Commentary* adopts the baseline definition of mobile device from NIST Special Publication 800-79-2 as that most consistent with the needs and expectations of electronic discovery practitioners, but refines it with four supplemental prerequisites. A mobile device, for the purpose of this *Commentary*, is a portable computing device that: (i) has a small-form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local data storage; and (iv) includes a self-contained power source. Mobile devices may also have voice-communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.[8]

While each of the four attributes set forth in the above NIST definition is a necessary condition to qualify as a mobile device, this *Commentary* applies the following additional limitations to its definition:

- Pure Internet of Things (IoT) devices (e.g., smart home assistants/hubs) are excluded from the definition of mobile device;[9]
- The primary purpose of the device must be for communication or content creation; and
- The device must not run an operating system generally associated with desktop and laptop computers for which other Sedona guidance is more directly applicable (e.g., Windows or MacOS).

Most smartphones and iOS/Android tablets satisfy the NIST definition as well as the three additional limiting factors enumerated above and therefore constitute mobile devices under this *Commentary*. Smart watches and e-readers, by contrast, are generally intended primarily for content consumption and accordingly would not be directly subject to the guidance in this *Commentary* (although much of the guidance may still be instructive where discovery of such devices is at issue).

Mobile device data is ESI that is stored on or accessible from a mobile device. Examples of mobile device data that may be stored on a mobile device include text messages (i.e., Short Message Service (SMS) messages, Multimedia Messaging Service (MMS) messages, Rich Communication Service

---

7 These definitions are aggregated in NIST's *Computer Security Research Center Glossary*, *available at* https://csrc.nist.gov/glossary/term/mobile_device.

8 HILDEGARD FERRAIOLO ET AL., *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*. NIST SP 800-79-2 (U.S. Department of Commerce, National Institute of Standards & Technology 2015), available at http://dx.doi.org/10.6028/NIST.SP.800-79-2.

9 Further guidance on the discovery of the Internet of Things will be addressed in a forthcoming Sedona Conference publication, *The Sedona Conference Primer on the eDiscovery Implications of the Internet of Things*.

(RCS) messages, and iMessages); voice messages; call logs/histories; contacts; calendar entries; appointments and reminders; location data (e.g., GPS coordinates and location history); photographs, videos, and other media files; downloaded files; deleted files; notes; locally stored passwords; internet browsing history; documents; local-application data; and raw data stored in the device's memory.

Mobile device data may also include cached emails and data from applications that are either stored on the device or accessible through connected accounts (e.g., emails, chats, and other files stored within Microsoft 365, Google Workspace, Slack, company servers, or other cloud-based platforms). However, the mobile device may not be the primary source for discovery of this type of data.

These are only current examples. Mobile devices and related systems and applications are constantly evolving. Accordingly, the guidance that this paper provides with respect to discovery of mobile devices and mobile device data is based on the current characteristics that generally define mobile devices and mobile device data set forth herein.

III. SCOPE OF DISCOVERY FOR MOBILE DEVICE DATA

Whether mobile device data may be subject to discovery in connection with federal litigation is governed by the Federal Rules of Civil Procedure. That is, the mobile device data must be relevant, not privileged, and proportional to the needs of the case.[10] However, a party generally need not provide discovery of mobile device data that is outside the party's possession, custody, or control, or that it identifies as not reasonably accessible due to undue burden or cost.[11] Mobile device data need not be admissible in evidence to be within the scope of discovery.[12]

In assessing whether mobile device data may be subject to discovery, the parties should consider the nature of the claims and defenses at issue and the potential relevance of the mobile device data thereto, as well as the following factors bearing on proportionality: the amount in controversy, the parties' relative access to the information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense outweighs its likely benefit.[13]

Factors that may inform these decisions include: (i) whether the party is an individual or corporation; (ii) the role and responsibilities of the individuals involved; (iii) where the relevant mobile device is located; (iv) whether the relevant data resides only on or is accessible exclusively from a given mobile device, or accessible from multiple sources (e.g., cloud accounts or other storage); and (v) which source is more reasonably accessible. Every situation should be assessed on its own terms, and the fact that some mobile device data might be accessible from another source does not mean that the mobile device is immune from discovery, including preservation requirements.[14]

Where an organization is involved, practitioners should consider whether and to what extent mobile devices were used within an organization to communicate about or conduct business, and whether the mobile device data stored on or accessible from those devices is considered to be within the organization's possession, custody, or control.[15] Questions that may inform these inquiries include:

---

10 FED. R. CIV. P. 26(b)(1).

11 *Id.*

12 *Id.*

13 *Id.*

14 FED. R. CIV. 26(b)(1), 26(b)(2)(B); *See The Sedona Principles, Third Edition*, *supra* note 1 at 56, 67, 71, 93, 95–97, 134–36 (Principles 1, 2, 3, 5, and 8); The Sedona Conference, *The Sedona Canada Principles Addressing Electronic Discovery, Third Edition*, 23 SEDONA CONF. J. 161, 180–190, 264, 270–71 (2022) (Principles 1, 2, and 8).

15 Further guidance on assessing whether discovery is within a party's possession, custody, or control is set forth in *The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control."* 25 SEDONA CONF. J. 1 (2024) [hereinafter *Commentary on Rule 34 and Rule 45*].

- Whether the individuals whose devices may be at issue are current or former employees, named parties, or otherwise receiving payment from the organization;[16]

- Whether the individuals who possess or control the data are officers, board members, or other agents of the organization;[17]

- Whether the individuals have or had a fiduciary relationship with the organization;[18]

- Whether the records sought from the individual's mobile device are the type of records to which the organization would likely have access, or request in the normal course of business;[19]

- Whether there is an employment contract, severance or other agreement, or company policy that requires the individual to provide materials or otherwise cooperate with company investigations or litigation;[20]

---

16 *Id.* at 45–49; Chevron Corp. v. Salazar, 275 F.R.D. 437, 448-49 (S.D.N.Y. 2011) ("Courts have repeatedly found that employers have control over their employees and can be required to produce documents in their employees' possession."); Canton v. Hoaglin, No. CIV A 2:08-CV-200, 2009 WL 1687927, at *3 (S.D. Ohio June 12, 2009) (collecting cases); *In re* NASDAQ Mkt.-Makers Antitrust Litig., 169 F.R.D. 493, 530–31 (S.D.N.Y. 1996) ("Plainly [Defendant's] employees are persons within its control" (quoting Herbst v. Able, 63 F.R.D. 135, 138 (S.D.N.Y. 1972)); *In re* Folding Carton Antitrust Litig., 76 F.R.D. 420, 423 (N.D. Ill. 1977) ("While the right to withhold payment does not ipso facto mean that defendants will be able to procure the documents, it is clearly an indicia of control); *see also* Goldstein v. Denner, 310 A.3d 548, at *580 (Del. Ch. Jan. 26, 2024) (held defendants had control over employees' personal devices, but not that of employee who departed one year before the duty to preserve arose)

17 *See, e.g.,* Flagg v. City of Detroit, 252 F.R.D. 346, 353–54 (E.D. Mich. 2008) ("courts have found that a corporate party may be deemed to have control over documents in the possession of one of its officers or employees." (citing Riddell Sports Inc. v. Brooks, 158 F.R.D. 555, 559 (S.D.N.Y. 1994); when materials are "created in connection with the officer's functions as a corporate employee, the corporation has a proprietary interest in them and the officer has a fiduciary duty to turn them over on demand.")); *id.*at 354 ("The courts also have held that documents in the possession of a party's agent—for example, an attorney—are considered to be within the party's control" (citing, inter alia, Comm'l Credit Corp. v. Repper (In re Ruppert), 309 F.2d 97, 98 (6th Cir. 1962); ASPCA v. Ringling Bros. & Barnum & Bailey Circus, 233 F.R.D. 209, 212 (D.D.C. 2006)); Miniace v. Pac. Martime Ass'n, No. C 04-03506 SI, 2006 WL 335389, at *2 (N.D. Cal. Feb. 13, 2006) (holding that fact that members of board of directors can easily be removed satisfies standard for control over current members; *but see In re* Pork Antitrust Litig., No. 18-CV-1776 (JRT/HB), 2022 WL 972401 (D. Minn. Mar. 31, 2022) at *6–7 (finding that Hormel did not have "control" over text messages on personally-owned mobile devices)

18 Royal Park Invs. SA/NV v. Deutsche Bank Nat'l Tr. Co., No. 14-CV-04394-AJN-BCM, 2016 WL 5408171, at *6–7 (S.D.N.Y. Sept. 27, 2016) (citing *Riddell*, 158 F.R.D. at 559 (where documents were created by corporate officer in connection with his functions as such, he "has a fiduciary duty to turn them over on demand")).

19 *In re Pork*, 2022 WL 972401, at *7 (requiring evidence that in the ordinary course of business, the party would seek, need, or expect to gain access to the mobile device data at issue).

20 *See e.g.,* H.J. Heinz, Co. v. Starr Surplus Lines, Ins. Co., No. 2:15-cv-00631- AJS, 2015 WL 12791338, at *4 (W.D. Pa. July 28, 2015) (finding Heinz had control over personal mobile devices because its BYOD policy stated that Heinz owns the property on the device and can delete content from devices in its sole discretion), *report and*

- Whether there is a history of the individual's cooperation in the litigation, such as attending a deposition or being represented by the organization's counsel;[21]

- Whether the party asked the individual for the mobile device or access to the mobile device data;[22]

- Whether the data is stored on an organization-issued or owned device;[23]

- What the organization's policies or procedures are for handling mobile devices when an employee leaves the organization;

- Whether the organization has a Bring Your Own Device (BYOD) policy, what its terms are, and the organization's history of enforcing the policy;[24]

---

recommendation adopted, No. 2:15-CV-00631-AJS, 2015 WL 12792025 (W.D. Pa. July 31, 2015); *Flagg*, 252 F.R.D. at 353–54 ("contractual provisions that confer a right of access to the requested materials" establish control) (citing Anderson v. Cryovac, Inc., 862 F.2d 910, 928–29 (1st Cir. 1988); Golden Trade, S.r.L. v. Lee Apparel Co., 143 F.R.D. 514, 525 (S.D.N.Y. 1992)).

21 *See, e.g., Royal Park*, 2016 WL 5408171, at *6–7 (citing as a factor non-party's past history of cooperating with document requests" (citing Alexander Interactive, Inc. v. Adorama, Inc., No. 12 CIV 6608 PKC JCF, 2014 WL 61472, at *3 (S.D.N.Y. Jan. 6, 2014)); *see also In re Pork*, 2022 WL 972401, at *3–4 (considering "whether the prior history of the case demonstrates cooperation by the non-party, including the production of documents and other assistance in conducting discovery"); *In re* NASDAQ Mkt.-Makers Antitrust Litig., 169 F.R.D. at 530–31 (current or former employee may be under party's control where, for example, that employee was (1) briefed by a company representative before or after being deposed in related matter; or (2) represented by company counsel or counsel paid by company).

22 *See, e.g., Royal Park*, 2016 WL 5408171, at *6–7; Exp.-Imp. Bank of U.S. v. Asia Pulp & Paper Co., Ltd., 233 F.R.D. 338, 341 (S.D.N.Y. 2005) ("courts insist that corporations, at the very least, ask their former employees to cooperate before asserting that they have no control over documents in the former employees' possession."); Uniden Am. Corp. v. Ericsson Inc., 181 F.R.D. 302, 307–08 (M D.N.C. 1998) ("there is no indication that defendant Ericsson has even made a request for these documents from [non-party affiliate] Ericsson Mobile"); *In re* Folding Carton Antitrust Litig., 76 F.R.D. 420, 423 (N.D. Ill. 1977) ("At the very least, defendants should make inquiry of such former employees. This is especially true where, as here, defendants do not assert that the former employees are unwilling or unable to cooperate."); Grace Bros. Ltd. v. Siena Holdings, Inc., No CIV.A 184-CC, 2009 WL 1547821, at *1 (Del. Ch. June 2, 2009) (granting motion to compel defendant Siena to produce emails "between members of Siena's board of directors" where Siena "failed to even ask that the directors look for any relevant emails in their accounts").

23 *H.J. Heinz Co.*, 2015 WL 12791338, at *4 (Heinz maintains custody and control over employee personal mobile devices which are company owned).

24 *See Commentary on BYOD, supra* note 5 at 528 ("It should come as no surprise that ESI that falls within the scope of discovery is often stored on mobile devices. Organizations cannot ignore their discovery obligations merely because a device containing unique, relevant ESI is also used for personal purposes.").

- Whether the organization knowingly lets employees use their personal devices, or is reasonably aware that its employees are using their personal devices to communicate about or conduct business;[25]

- Whether the organization uses any other tools to monitor or access data on an employee's mobile devices.

These factors are illustrative of those that courts consider, and the weight courts may ascribe any particular factor typically depends on the circumstance of the case. Additionally, this *Commentary* does not intend to suggest that any one factor should be afforded greater or less weight in a party's consideration or determination of the relevant of mobile device discovery.

BYOD policies may address the questions above and may inform the extent to which an organization is determined to have control over or access to an employees' mobile devices. While BYOD policies will necessarily vary from organization to organization, and no one factor is determinative, individually, or in combination, courts typically consider the following in assessing an organization's control over employee mobile device data—whether a BYOD policy: (i) requires employees to cooperate with company requests for information on or access to mobile devices in their possession; (ii) specifies that the organization retains ownership of or control over any business information on an employee's personal device at all times; (iii) permits employees to use personal devices for company business and to access company systems in exchange for the organization's right to obtain the device or access or collect data on the device on demand; (iv) states that an employee waives any rights or expectations of privacy with respect to their personal devices or data on those devices; or (v) requires employees to waive any rights or expectations of privacy as a condition of using the device to communicate about company business or access company systems; and (vi) if the policy is silent on giving an organization access to the employees' mobile device, and to personal content on the mobile device.[26]

---

[25] *See Denner*, 310 A.3d at *573 ("Business related texts on employee personal devices are likewise within an organization's possession, custody, or control."); Miramontes, 2023 WL 3855603 ("the Court finds persuasive Miramontes' evidence that Peraton did not issue company cell phones and Peraton employees regularly conducted business on their cell phones. Under these circumstances, the Court finds Peraton had control over the text messages. . .."); Colonies Partners, L.P. v. Cty. of San Bernardino, No. 5:18-cv-00420-JGB (SHK), 2020 WL 1496444 (C.D. Cal. Feb. 27, 2020) ("although the County did not necessarily have direct access to the personal emails and text messages, Ramos was an employee of the County engaging in County business and business that implicated Plaintiffs on his devices and campaign email. Additionally, as a Defendant in the case, and defending Ramos—an employee—and responsible for any potential judgment in Plaintiffs' favor, a duty to preserve ESI can be imputed to the County."), *report and recommendation adopted*, 2020 WL 1491339 (C.D. Cal. Mar. 27, 2020); *see also* Alter v. Rocky Point Sch. Dist., No. 13-1100 JS AKT, 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.").

[26] *In re Pork*, 2022 WL 972401 (employer did not have control over employees' personal devices where BYOD policy: (i) allowed employees to use their personally-owned cell phones to access company systems and specified that the company retains ownership of all "data that is sourced from Hormel systems and synced between the mobile device and its servers"; and (ii) gave Hormel the ability to wipe personal data from a personally-owned device by resetting

The extent to which organizations use Mobile Device Management (MDM) tools to monitor, back up, or archive data on mobile devices used by their employees may also inform the extent to which it has access to or control over an employee's mobile device data. On the other hand, even where mobile device data associated with MDM tools, archives or cloud backups are accessible by the organization, such data may be more readily accessible from the mobile device, if the primary source becomes unavailable, or if there are syncing issues or gaps in the data available from the MDM tools, archives or cloud back-ups.[27]

Given the potential complexity of identifying, preserving, and collecting mobile device data, it is often advisable to meet and confer with opposing parties early in a matter and attempt to reach consensus on mobile device data that will be considered in-scope for the matter.[28]

it to a factory floor state and employee could restore personal data that was backed-up, but not assert employer ownership over text messages).

[27] For more information about the applicable standards governing the determination of a party's possession, custody or control over discovery, *See Commentary on Rule 34 and Rule 45, supra* note 15; *See Commentary on BYOD, supra* note 5 at 495; *See The Sedona Principles*, *Third Edition, supra* note 1.

[28] The Sedona Conference, *Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009 Supp.); *See The Sedona Principles, Third Edition*, *supra* note 1 at 71–72, 75, 76–78 (Principle 3).

IV. GUIDANCE FOR IDENTIFYING RELEVANT MOBILE DEVICE DATA SOURCES

There is no bright-line rule for how parties and counsel must conduct their investigation to identify the mobile device data that may be subject to discovery. However, parties and counsel should undertake all reasonably appropriate measures to identify individuals who may have relevant information stored on or accessible from their mobile devices, whether business or personal. Parties and their counsel should consider adopting a broader view as to the mobile devices potentially in scope, so as not to risk potentially relevant data being lost or destroyed.

One common investigative tool used to identify the mobile device data potentially in scope for a matter is written questionnaires regarding the potential mobile devices and mobile device data at issue. But further investigation, custodial interviews, and, where corporate parties are involved, interviews with IT and other personnel with knowledge of a company's policies and procedures governing the issuance, use, monitoring, storage, and archiving of mobile devices and mobile device data is often advisable and may be required.

Custodial interviews involve directly engaging with those individuals who possess or have control over the mobile devices under investigation. These interviews should seek to identify all mobile devices that may contain discoverable information, where the relevant devices and data are located, and whether the relevant mobile device data exists only on the mobile device or in other locations. These interviews should also identify any potential issues with the preservation, collection, or production of relevant data from those devices.

Depending on the facts and circumstances of the case, the following are topics that may be considered in a custodial interview, whether through written questionnaires, custodial interviews, or a combination of the two:

- What types of mobile devices the individual used during the relevant time period;
- What relevant data each device may contain (e.g., emails, text messages, documents);
- What applications or communications tools installed on the devices were used to store or communicate the relevant information;
- Whether data was ever transferred from one device to another;
- Whether the party still has the mobile device(s) in question, and if not:
    - What happened to the device(s);
    - When; and
    - Was any data transferred to a new device or backed up prior to its loss/disposition, and if so when.

- Whether any security methods or encryption were used on the device, including whether access to the device is managed via passcode, password or biometric methods;

- If relevant to the legal matter, whether location services or other features that track location or movements are or were enabled;

- The make and model of the devices, the operating system installed, and the service provider;

- How mobile device data is stored (e.g., locally v. cloud, etc.);

- Whether data is or was synced between the mobile device and other devices (e.g., computers, cloud accounts, etc.), the frequency, and the method(s) or tool(s) used;

- How the individual typically handles data preservation, including whether s/he regularly backs up data from the mobile device(s), how often, and where;

- Whether the individual used mobile devices in a manner that created or captured information or data relevant to the litigation during the relevant period; and

- How the individual typically handles deletion of data on the mobile device, including auto-delete settings in place during the relevant period, whether any data was manually deleted, and under what circumstances.

- Where a corporate party is involved, counsel should also endeavor to learn:

- Whether employees used mobile devices to communicate about or conduct business during the relevant period;[29]

- Whether any software applications or communication tools installed on those devices were used to communicate about or conduct business or communicate about the claims or defenses in the litigation;[30]

- Which employees used such mobile devices;

- Whether the employees are current or former employees;

- Whether the mobile devices used were company-issued or personal devices;

- Whether the company is in possession, custody or control of the devices at issue;

---

29 *See supra* note 21

30 *Id.*

- Whether the company has or had any bring your own device policies or other acceptable-use policies or procedures in place governing the employees' use of mobile devices, including personal devices, to communicate about or conduct business, and the scope of those policies in terms of defining an employer's possession, custody or control over and ability to access data on mobile devices subject to such policy;

- To the extent personal devices were used to communicate about or conduct business, whether the organization was aware of such use;

- Whether mobile device management tools or container software were used on the mobile device;

- Whether any back-up systems or procedures were in place to back up or archive data on the mobile device; and

- Whether any offboarding procedures were employed to preserve mobile device data on the personal devices of departing employees.

Another tool parties may use to help identify and assess whether discoverable mobile device data may be subject to discovery is to sample such data. Sampling can be performed in a variety of ways, from the custodian under the direction of counsel searching his/her mobile device for potentially relevant data, counsel reviewing sample data from a potential custodian's device(s), collecting a potential custodian's physical device(s) and running searches across the device, and forensically collecting data on a potential custodian's mobile device and running searches across the data.

Once a party has identified the mobile devices and mobile device data that may contain relevant information, and where that information is located or stored, it can better assess what its obligations are to preserve, collect and produce data from these sources.

Additionally, Rule 26(f) of the Federal Rules of Civil Procedure requires parties, at the outset of a matter, to discuss the preservation, disclosure, and discovery of ESI, which necessarily includes identifying relevant data sources—both within and outside of the party's possession, custody, or control of the party. Rule 26(b)(2) also requires the parties to identify any data sources it believes to be not reasonably accessible due to undue burden or cost. Identifying and conferring about data sources is important for the efficient conduct of the litigation and serves Rule 26's aim of identifying and addressing issues concerning the preservation, disclosure and discovery of ESI early in the litigation. Among other things, it allows parties to understand the potential sources of relevant documents and information in the case, and actions they may need to take to obtain or ensure relevant data is preserved for litigation and may help minimize disputes down the line. For example, if a party states that it does not have possession, custody or control over relevant mobile device data, the opposing party may elect to issue preservation letters or non-party subpoenas to the individuals or entities in possession, custody or control of the relevant mobile devices or data. Additionally, the parties may

reach agreement regarding the relevant mobile devices and mobile device data that will be preserved and how.

These disclosures are especially important with respect to mobile devices and mobile device data given their prolific use and potential for loss or destruction.

V. GUIDANCE FOR DETERMINING HOW TO MEET PRESERVATION OBLIGATIONS FOR MOBILE DEVICES.

The obligation to preserve mobile device data is no different than the obligation to preserve other types of ESI and requires a party to make reasonable and good-faith efforts to preserve potentially relevant information. A party's preservation obligations and efforts are assessed on a case-by-case basis and must be reasonable under the circumstances.

In evaluating what preservation steps are reasonable with respect to a particular mobile device, the inquiry typically begins with an investigation into the scope of discoverable information stored on or accessible from the device. As discussed above in Section 4, this investigation may include interviews with the custodian of the device, other knowledgeable individuals, legal staff, and data stewards. Parties must also be cognizant that this analysis must be ongoing and dynamic because "[p]reservation obligations may expand, or contract, as the contours of claims and defenses at issue are clarified during the pendency of a matter."[31]

Preservation decisions should be guided by a fact-based understanding of the sources and types of discoverable data on the device and may consider the location and accessibility of the devices and data in question. Additional considerations may include the likely volume of discoverable data, its uniqueness, and available techniques for preservation along with associated costs and burdens.

A. Preservation Methodologies

Mobile device preservation methods exist on a continuum and can vary greatly in terms of effectiveness and cost. For example, one preservation method includes sending a well-drafted legal hold notice to the potentially relevant custodians with clear instructions about how to preserve discoverable mobile device data. This type of preservation involves minimal cost and burden to the party. But there is a risk that despite, or even because of, the hold notice, the data could be lost in any number of ways. The custodian receiving the notice, may, for example: not understand the legal hold instructions; ignore the instructions; not know how to preserve the data (e.g., back up to the cloud or remove auto delete), lose the device; break or damage the device; exchange the device without taking necessary steps to back up or transfer the relevant data; perform a factory reset of the device; and accidentally or even deliberately delete content. If the party itself does not take affirmative steps to ensure compliance with the litigation hold instructions, the litigation hold notice may be considered inadequate to satisfy the party's preservation obligations.

At the other end of the preservation continuum, a party may engage a professional to perform a forensic collection of the device using advanced software and tools. Collecting to preserve can significantly minimize the risk of data loss but can be relatively costly depending on the data sources, volume of data, method of collection, available tools, and party involved.

---

31 *See The Sedona Principles, Third Edition, supra* note 1.

Other preservation options include having the mobile device set to back up to its associated cloud storage repository (e.g., Apple's iCloud, Samsung Cloud, etc.), sequestering and securely storing the device itself, copying specific files from the device to an accessible location, or even temporarily discontinuing use of the device. Finally, if available, preservation can be managed by use of MDM software, by limiting an individual's access to data on the device that is managed by the MDM software.

In addition to the monetary expense, scheduling and coordinating a collection process involving the vendor performing the collection, the custodian, and counsel, can be time consuming; the custodian may be without their device for hours, days, or even weeks depending on technological issues and logistics; the collection process may not allow for targeting specific, discoverable data and may require collection of the full device, including irrelevant and personal content; and the collected data can be voluminous and challenging to process, cull, review, and produce to an external location (e.g., cloud repository, server, drive, or other location). However, technological advancements, including the ability to collect mobile device data remotely, may mitigate some of these concerns.

Additional factors to consider in determining appropriate preservation methods include the technical proficiency of the parties and individual custodians, whether the mobile device data is stored only on the mobile device itself, whether it is synchronized with other data sources, such as a cloud-based backup or an enterprise system, and whether the data might be subject to deletion either because of automated processes designed to manage the memory space available on the device or through actions by the user. For example, sophisticated parties may be held to a higher standard for preservation of mobile devices and mobile device data than less sophisticated litigants.[32] Even when the mobile device is managed by a corporate party's IT department, however, preservation can still be challenging because there may be relevant information that is unmanaged, such as location data or other information that uniquely resides on the mobile device.

Less sophisticated litigants or custodians may be more likely to lose mobile device data for various reasons, including failing to turn off auto-delete messaging settings, not having cloud backup enabled, and using devices that are logged into others' accounts. Counsel should evaluate their client's level of sophistication when providing guidance on the appropriate methods for mobile device data preservation. When dealing with less sophisticated individuals, parties and counsel may also consider

---

[32] FED. R. CIV. P. 37(e) advisory committee's notes to 2015 amendment ("The court should be sensitive to the party's sophistication with regard to litigation in evaluating preservation efforts; some litigants, particularly individual litigants, may be less familiar with preservation obligations than others who have considerable experience in litigation."); *In re* Google Play Store Antitrust Litig., 664 F. Supp. 3d 981, 982 (N.D. Cal. 2023) (holding Google to a higher standard as a "frequent and sophisticated litigation party"); Matter of *In re* Skanska USA Civ. Se. Inc., 340 F.R.D. 180, 189 (N.D. Fla. 2021) (held fact that "Skanska is certainly far from being an unsophisticated litigant" relevant to determination of its intent in failing to preserve relevant ESI); Living Color Enters., Inc. v. New Era Aquaculture, Ltd., No. 14-CV-62216, 2016 WL 1105297, at *6 (S.D. Fla. Mar. 22, 2016) (finding defendant only acted negligently in failing to preserve relevant text messages, in part because he "is an individual who appears to be a relatively unsophisticated litigant."); Harkabi v. SanDisk Corp., 275 F.R.D. 414, 419 (S.D.N.Y. 2010) (describing defendant's "size and cutting-edge technology [as] rais[ing] an expectation of competence in maintaining its own electronic records").

whether it is preferable to collect mobile device data as soon as possible to avoid potential spoliation issues.

Ultimately, if a party has a duty to preserve mobile device data (because it is deemed within their possession, custody or control), parties should weigh the costs and benefits of available preservation methods in determining which method is appropriate to meet its preservation obligations for the matter. A party must also be mindful that its preservation obligations, including the appropriate preservation method, may be subject to change, for example, as the matter progresses and more information becomes known or discovery requests are served, among other things.

B. Cooperation and Transparency: Managing Expectations

Because mobile device data presents numerous factors and challenges for preservation, some level of transparency into the methodologies used to preserve mobile- device data and cooperation among parties and their counsel may be necessary to manage expectations, and in the best interests of the parties to address the dual concerns that relevant data is adequately preserved, while mitigating potential concerns about costs and associated burdens. For a further discussion of the different preservation challenges mobile device data presents, see Section VI *supra*.

Additionally, involving the requesting party early in preservation discussions may also help lessen the burden on the preserving party at the collection, search, review, and production stages (see Sections VI, VII and VIII below).

VI. GUIDANCE ON THE FACTORS PARTIES AND COURTS SHOULD CONSIDER WHEN COLLECTING MOBILE DEVICE DATA FOR LITIGATION

The selection of an appropriate mobile-data collection method depends on various factors, including the nature of the matter and the relevant mobile device data at issue, how it is stored or accessed, the type of applications used, the way the custodian interacts with their mobile device, and whether the data may be accessed more easily from other sources. For example, where the relevant mobile device data to be collected is synced to enterprise applications (e.g., Microsoft Exchange), or concerns applications that store data in the cloud (e.g., Gmail), a party may consider whether such data can be collected more easily from those other sources, and whether collection from the physical mobile device is required. On the other hand, there are some types of data, such as location data, call histories, contacts, photos, and even some locally stored messaging data, that are typically only available from the mobile device itself. When it is necessary to collect data from the mobile device, the method of collection selected is crucial for gathering data effectively while ensuring its integrity and admissibility in legal proceedings.

The process of collecting mobile evidence typically involves various techniques tailored to the specific devices and applications involved. Before collection takes place, custodial interviews and IT interviews can offer unique insights into the usage patterns and content present on mobile devices.[33]

Four primary methods exist to collect mobile device data, including, in decreasing order of complexity and completeness: (i) comprehensive data extraction; (ii) logical extraction; (iii) cloud-based collection; and (iv) targeted manual collection. There are pros and cons to each method and selecting a reasonable and defensible method for the action will depend on a variety of factors, including cost, burden, importance of the data, and availability from other sources. Further, the collection method and tool selection can have an impact downstream. For example, some collection methods and tools will impact the format available for production. Where appropriate, it is advisable to discuss the collection options available with a forensic analyst, including how the collected data will be presented for review and formatted for production.

A. Forensic Image Collection

Forensic-image collection is a method that captures a full-file system image (i.e., bit-for-bit copy) of accessible data stored on a mobile device.[34] In other words, a full-file system image will capture all

---

33 *See* Section IV, p. 6–8.

34 A forensic image of a mobile device is different from a forensic image of a hard drive. The latter is a complete bit-for-bit copy of all data on a computer hard drive, including deleted files and slack space (i.e., drive sectors with no content). In contrast, a forensic image of a cell phone captures similar data but involves added complexities due to different storage locations, app data, and sophisticated encryption requiring specialized tools for effective analysis. Essentially, extracting data from a cell phone is more intricate than from a standard hard drive. *See, e.g.*, Dale Liu, *Digital Forensics and Analyzing Data* (ScienceDirect 2009), https://www.sciencedirect.com/topics/computer-

data on the mobile device that can be captured, including pictures, videos, chat histories, application data, location data, internet evidence, and deleted content. Note that all data on every mobile device is available for collection. Security settings and encryption, for example, may make some data unavailable even for a full-file system image.[35] Nevertheless, comprehensive data extraction provides forensic examiners with the most comprehensive view of the device's contents compared with other collection methods.

This collection method also preserves evidence in its original state, maintaining its integrity and admissibility in legal proceedings, and ensures that no potentially relevant evidence is missed, altered, or tampered with during the investigation process. However, physical access to the device is required.[36] Additionally, forensic-imaging software enables the forensic examiner to create a variety of reports, including one on the device's installed applications, potentially facilitating the identification of previously unidentified applications that may be pertinent to the matter.

Full-device imaging may be warranted where data is exclusively available on the device (and cannot be obtained from remote servers or cloud repositories), or where deleted or fragmented data are potentially relevant to the litigation or investigation.

B. Logical Collections

Logical extraction is the process of collecting data from a mobile device by communicating with the device's operating system using an Application Programming Interface (API). Unlike comprehensive data extraction, logical extraction does not include a bit-by-bit copy of the mobile device, and typical logical-extraction tools cannot recover deleted files or be used on a locked device. Like a comprehensive data extraction, logical extractions generally require physical access to the mobile device,[37] although there are emerging technologies that enable a true remote collection over the Internet with no physical connection to the mobile device. Logical-extraction methods are commonly used in civil proceedings where additional data that can only be acquired through a comprehensive data extraction is not relevant to the claims or defenses at issue, or temporarily taking possession of the device

---

science/forensic-image# (last visited Jan 28, 2025); *Acquisitions* (Science Direct 2009), https://www.sciencedirect.com/topics/computer-science/forensic-image# (last visited Jan. 28, 2025).

35 Deleted data is the most common type of data on a mobile device that may not be available for collection, depending on the type of encryption used on the device. Encryption and decryption technologies are constantly evolving, but it is important to understand that there may be data on a mobile device that simply cannot be captured from the device. Note that data that is inaccessible on a mobile device may be available elsewhere, such as a cloud backup or on an older device.

36 Note that many forensic analysts refer to a "remote" collection, but that is actually a misnomer, referring instead to an option to perform a collection without the forensic analyst physically present. It is increasingly common for the forensic technician to ship a collection device (such as a laptop computer) to the custodian and then perform the collection during a video conference, guiding the custodian through the process of connecting the mobile device to the collection device and then passing control to the forensic analyst.

37 *See* 36, *supra.*

is not required to collect the relevant data. As such, costs are typically lower and disruption to the device owner's use of the device is minimized.

However, there may be times where a logical collection may not be sufficient to satisfy a party's discovery obligations. For example, there may be circumstances where data that is typically more readily accessible from a host server (such as an email server or messaging service) is inaccessible due to technical issues or legal constraints. In such cases, the device may be the only source of the available data, and a comprehensive physical collection may be the best way to ensure the collection is as complete as possible. Similarly, if it is important to collect data that is only cached on the mobile device, a comprehensive physical collection may be the only way to identify and collect the complete data stored on the device. For example, it may be important to identify and collect email from a mobile device to prove that the email was actually delivered to the device. Depending on the configuration of the email application being used, the type of device and its operating system, full emails stored on the device may not be available for logical extraction and may only be available for collection via a full-file system extraction using appropriate forensic software. Likewise, certain chat messages may be cached on the mobile device even when they are no longer stored on the cloud application hosting the messaging service. In such cases, a collection via comprehensive data extraction from the device ensures the retrieval of these messages for forensic analysis.

If the device and operating system support it, a targeted collection of specific types of data, e.g. only text messages, or only certain types of data, may be an option with logical extraction.

C. Forensic Cloud Collection

Forensic cloud collection is technically not a mobile device collection, as it refers to the process of gathering data that is synced between a mobile device and the operating system or application platform's cloud service, rather than from the device itself. Forensic cloud collection may be a reasonable method for collecting data such as email and chat messages sent via messaging applications like Slack and Microsoft Teams that is stored on external servers, or in cloud repositories, and can typically be collected from those sources without obtaining the device itself. Additionally, if the data to be collected is backed up to the cloud, forensic cloud collection methods may also be appropriate, and less disruptive to the ongoing use of the mobile device by its user. Likewise, where the physical device is not available for collection, but there is a cloud backup, forensic cloud collection may be appropriate. However, there are instances where using forensic cloud collection to collect messages and other data may not be reasonable and collection from a mobile device is necessary.

Forensic cloud collection typically requires specialized expertise with the legal, technical, and privacy challenges associated with accessing data stored in the cloud. Obviously, forensic cloud collections are only possible where the device has been configured to back up to the cloud, and the content available may be limited based on the mobile device and application settings and the cloud backup configuration, including storage limitations.[38]

---

[38] For example, WhatsApp requires specific settings to be enabled on the device to allow backup of chat messages.

D. Non-Forensic Targeted Manual Collection

Targeted, non-forensic manual collections typically do not involve the use of forensic collection tools and are used to collect a limited set of mobile device data. Examples of targeted manual collections include screenshots of text messages or individual files collected manually. Because targeted manual collections do not utilize forensic tools, metadata associated with the mobile device data will not be obtained and is incapable of being produced. Accordingly, targeted manual collections may raise certain evidentiary and other concerns.[39]

Nevertheless, a party may decide that targeted collections are reasonable in certain situations where the metadata will not be at issue or a forensic collection is not proportionate to the needs of the case. Parties considering targeted, non-forensic manual collection should also consider whether it would be appropriate or beneficial to seek agreement with the opposing party, as the lack of original metadata could adversely impact the ability to authenticate the documents collected.

E. Special Consideration for Collections Involving Encrypted Data

Special consideration may be required for collections involving encrypted applications like WhatsApp or Signal, as currently available collection tools may not be capable of collecting such data in a reasonably usable form. For example, while encrypted messages may be collected using commercially available tools, the encryption may make them unusable. The type of mobile device, the mobile device's operating system and the version of the operating system installed may also affect a party's ability to collect encrypted data. Manual collection via screenshots or other methods may be the only means available for collection.[40]

F. Privacy Considerations for Mobile Collections

Depending on the circumstances, parties may need to consider certain privacy interests an individual may have in data on their mobile device in determining the appropriate method of collection.

Similarly, parties may need to consider applicable privacy laws such as the Health Insurance Portability and Accountability Act (HIPAA), European Union's General Data Protection Regulation (GDPR), China's Data Security Law, and other privacy regulations and requirements in determining the appropriate collection method. Such laws may raise obstacles to the collection of the data or require the collection to be performed a certain way, and that the relevant data be identified before any data is transferred to another jurisdiction. There may also be restrictions on the use of the data after it is collected.

---

[39] For a discussion of the authentication and admissibility of mobile device screenshots, *see* The Sedona Conference, *Commentary on ESI Evidence & Admissibility, Second Edition,* 22 SEDONA CONF. J. 83, 111–13 (2021).

[40] Applications that enable ephemeral messaging, such as Signal, Snapchat, Telegram, WeChat, WhatsApp, and Wickr, may come up in custodial interviews or otherwise. By definition, an ephemeral message that has been automatically deleted by the application would typically not be available for collection. For further information about ephemeral messaging, *see* The Sedona Conference, *Commentary on Ephemeral Messaging,* 22 SEDONA CONF. J. 435 (2021).

While a targeted manual collection may address such privacy concerns in certain situations by focusing only on specific data on the device, the completeness of such collections and limitations on metadata available may raise questions concerning the reasonableness of such collection methods. Additionally, there are strategies that can be employed post-collection to identify sensitive information and protect privacy concerns, including targeted keyword searches, regular-expression searches, and trained machine- learning algorithms.

In summary, the methods of collection for mobile evidence encompass a combination of custodial interviews and device-collection methods, each offering valuable insight into device-usage patterns and technical configurations. By employing these methods strategically, counsel can gather relevant evidence effectively while adhering to legal and ethical standards governing digital forensics investigations.

VII. GUIDANCE ON DETERMINING THE APPROPRIATE METHODOLOGY FOR SEARCHING MOBILE DEVICE DATA

Effectively searching mobile device data requires careful consideration of numerous factors to ensure a thorough and defensible approach.

A. Factors Influencing Search Methods

1. Initial Investigation

A party's (or counsel's) initial investigation into the types and volume of mobile device data at issue is crucial in developing an effective and defensible search methodology.[41] For example, if the investigation suggests that there is very little data on a mobile device that is potentially relevant, the party may consider whether less costly or burdensome search methods are appropriate. Such methods may include, for example, with respect to text messages, a user and/or counsel manually searching a phone for responsive text messages. However, such methods may not be sanctioned by courts, and carry significant risks, such as the relevant data not adequately being identified, or lost as a result of various storage and deletion settings or user action. By contrast, if the investigation suggests that there is likely a greater amount of potentially relevant data on a mobile device, a party may consider whether searching the mobile device data using more robust and reliable advanced search tools is appropriate.

By way of further example, the initial investigation, and in particular, custodial interviews, may identify relevant keywords, project names, code words, acronyms, or abbreviations that the party should apply if using keywords to perform its search, and which may be required to render the search reasonable and defensible. Likewise, the investigation may identify particular contacts, conversation participants, phone numbers or conversations that may need to be searched to identify relevant conversations and messages.

Additionally, it is important to learn through the initial investigation whether any potentially discoverable data is encrypted. Encryption can not only significantly impede extraction capabilities (e.g., without a user's password, a device may not even be capable of being unlocked for collection and search), but encrypted data is generally not searchable and will not be included in search results. Thus, it may be necessary to explore potential avenues to access encrypted data in investigations with proper authorization, while recognizing the importance of upholding user privacy rights and data-security best practices.

---

[41] Information gleaned from this investigation may reveal not only information relevant to selecting an appropriate search methodology, but also information about what mobile device data is likely to contain discoverable content, the scope of mobile device usage (e.g., business or personal), the time period at issue, and the volume of potentially discoverable content that may be relevant to determining the appropriate scope of a party's search.

While information obtained during custodial interviews may be used to guide a party's search, verification measures may also be warranted, and parties may need to undertake additional search efforts as matters develop.

2. Collection Methods

The means by which mobile device data is collected significantly impacts available search options. Available methods typically range from manual collection of screenshots and individual files to forensic extraction of all accessible data on a mobile device and/or collection of cloud backups. In some cases, the extracted data can be imported into a forensic tool for parsing of databases containing call logs, contacts, notes, and text messages, allowing more types of data to be searched in different ways. For example, data content can be searched using keywords, while structured metadata can be filtered for date ranges or other parameters.[42] On the other hand, if the collection consists only of screenshots or video captures, searching capabilities will be quite limited, though some technological tools may allow for extraction of text from screenshots or transcription of video content, enabling some forms of search.

3. Data Type and Electronic Discovery Tool Considerations.

To develop an appropriate search methodology, it is important to consider the type of data being searched and the electronic discovery tools being used. For instance, there may be limitations to running in-app searches of text message data, including the lack of advanced search operators like wildcards (e.g., "*") or proximity searching (terms appearing within a specific number of words from each other), and courts have rejected parties' attempts to develop their own search terms and run their own in-app searches on text-message data.[43] Likewise, many industry-standard, mobile forensic-collection tools lack support for such advanced search methods. To run keyword searches effectively, it may be necessary to export the collected data from the forensic tool into a review tool with more robust search capabilities. Similarly, some forensic-collection tools might not support transcription of media files like voicemails, audio recordings, or videos that are often found on mobile devices. This data must be loaded into a different platform that supports or has such transcription features integrated and can apply those tools before running keyword searches.

The manner in which chats are processed and viewed can also impact the reasonableness of the search method. For example, if each message in a chat is processed and viewed as an individual file (as opposed to being converted into a format where messages within the chat are grouped together as a thread), then exporting or reviewing only messages with keyword hits may also make it difficult for a reviewer to understand the context.

---

42 *See* Section VI.

43 *See* Witham v. Hershey Co., No. 23-CV-1563 (LMP/JFD), 2025 WL 444399, at *4 (D. Minn. Feb. 10, 2025) (held where plaintiff "developed search terms on his own and entered them into his text messaging application and took screenshots of the messages he thought were responsive" was "a hopelessly inadequate way to search for and produce documents responsive to an RFP in federal court").

Even the search tool can impact the effectiveness of the search. For instance, in chats, participants tend to speak more informally, using emojis and abbreviations, making typos, and sending messages with erroneously auto-corrected text. As a result, searches based on participants and date ranges are generally more effective for text messages, chats, and similar mobile messaging-type data, than keyword searches. By way of example, searching for "meeting" might miss messages or notes referring to a "mtg" or "meetup." These same issues may also limit the effectiveness of using search terms on other user-generated content on the mobile device such as memos, notes, and even transcribed media files. As a result, when dealing with these types of mobile data, relying solely on strict keyword searches can be ineffective and not reasonable or defensible. Using a fuzzy match search may help to mitigate this issue because it allows for variations in spelling and accounts for typos and user-generated abbreviations commonly found in mobile communications.

4. Advanced Analytic Tools

The use of various advanced analytics tools, such as machine learning, predictive coding, or other artificial intelligence-based tools, as well as regular-expression searches, and textual near-duplicate analysis, may also be considered as part of a party's search methodology. However, these methods may not always be suitable for effectively searching certain types of mobile device data, and due consideration should be given to the benefits and limitations of such tools, as applied to mobile device data, when assessing the reasonableness of a party's search and/or other methods that may be required to support or validate the same.

For example, mobile data such as text messages may be incomplete, or contain informal dialogue, abbreviations, acronyms, emojis, slang, and autocorrections that may not be suitable for advanced analytic tools like machine learning, predictive coding, or artificial intelligence-based tools, which often are premised on algorithms that analyze large volumes of text with conceptually related content. The often-smaller volume of mobile device data available may be insufficient to effectively train such analytic models.

Other search methods like regular-expression searches may be effective at searching for specific patterns within the data, like phone numbers, credit card numbers, Social Security Numbers, and other data defined by a fixed pattern (e.g., a regular expression can capture variations in phone number formats across different countries). However, their usefulness with mobile device data will depend on the prevalence of such structured terms in the collected data.

Textual near-duplicate analysis, which can help identify data with similar content, may also be helpful in ensuring that potentially responsive information is not overlooked because of the application of some other search process.

Data assessment and visualization tools can also be effective in searching and analyzing mobile device data. By searching across the metadata, these tools can identify communication patterns and potential anomalies. For example, creating network graphs of key players within a communication network helps identify who communicated most frequently with whom, information that might otherwise not be revealed with a traditional keyword search. Timeline visualizations can showcase

the flow of communication over time, potentially highlighting periods of increased or absent communication activity.

Finally, sampling can be effective in developing a search methodology. In some instances, sampling a representative subset of the mobile device data might be helpful in identifying the data types that can be effectively searched, developing appropriate search criteria, assessing the efficacy of searches, and verifying information provided by custodians. For example, sampling a custodian's text messages may identify additional keywords, participants, or phone numbers that the initial investigation did not identify. Likewise, sampling may identify additional data on the device not previously identified.

5. Cooperation/Transparency Related to Search Methodology

The producing party is generally considered to be "best situated to evaluate the procedures, methodologies, and technologies" to be used to satisfy its obligations to conduct a reasonable search.[44] However, courts generally expect some level of cooperation and transparency among the parties. Additionally, practitioners generally agree that cooperation and transparency in the discovery process should be encouraged.[45]

Given the unique nature of mobile device data, transparency and cooperation with respect to a party's search methodology early in the discovery process can aid in the development of effective searches and prevent unnecessary disputes.[46]

---

44 *See The Sedona Principles, Third Edition*, *supra* note 1, Principle 6, 118; *see, e.g.*, Hyles v. New York City, 10 Civ. 3119 (AT) (AJP), 2016 WL 4077114, at *4–5 (S.D.N.Y. Aug. 1, 2016); Hastings v. Ford Motor Co., No. 19- CV-2217-BAS-MDD, 2021 WL 1238870, at *2 (S.D. Cal. Apr. 2, 2021); *In re* EpiPen (Epinephrine Injection, USP) Mktg., Sales Pracs. & Antitrust Litig., No. 17-MD-2785-DDC-TJJ, 2018 WL 1440923, at *2 (D. Kan. Mar. 15, 2018).

45 *See The Sedona Principles*, *Third Edition, supra* note 1 at 126–27.

46 *Id.*, Principle 3; comment 3e at 37.

VIII. GUIDANCE ON DETERMINING THE PRODUCTION FORMAT FOR MOBILE DEVICE DATA

As reflected in the prior sections of this *Commentary*, the ubiquitous nature of mobile devices and the variability in how mobile device data is created, accessed, and stored in professional and personal spheres may present challenges for parties and their counsel in litigation. This is equally true in trying to determine appropriate format(s) for the production of mobile device data. Because those decisions may be both matter, custodian, and data-specific, this section focuses on the key facts and factors that parties and courts should consider in discussing the appropriate form or formats for the production of mobile device data.

While production format is normally considered one of the last steps in the process of producing ESI, a number of provisions in the Federal Rules require or strongly encourage an early discussion among counsel regarding production format. The discovery conference mandated by Rule 26(f) and the joint discovery plan required by Rule 26(f)(3) "must" include a discussion of discovery issues "including the form or forms in which [ESI] should be produced." To comply with these rules and make the Rule 26(f) conference a meaningful exercise, counsel for the parties should undertake a good-faith effort to understand what relevant mobile device data may be within their clients' possession, custody, and/or control, where mobile device data is located or stored, and a proposed format for those productions. Given the potential volume and variability of mobile device data, many parties typically benefit from accelerating an investigation of these issues to inform a discussion about how the parties will address them practically. Parties should consider whether to address these issues by reaching agreement on these matters in an ESI Protocol or Production Specification Protocol, entered into at the outset of the case.

Additionally, Rule 34 and the Advisory Committee Notes to the 2006 Amendments make clear that both the requesting and responding parties have a role in discussing and determining the form of production.[47]

Beyond the requirements of the Federal Rules, early discussions of the production format of mobile device data among counsel makes good sense for several practical reasons.

First, mobile devices generate a significant amount of data which can be stored in several locations including the device itself, in cloud storage, and backup systems, and the source of the data might impact the appropriate or available form of production. In some cases, mobile device data may need to be processed to a unique format to enable review.

---

47 *See* Rule 34 (b)(1)(C) and (b)(2)(D); Rule 34(b) advisory committee's note to 2006 amendment (stating the requesting party "may" specify a form of production, the responding party may object and "if the requesting party does not specify a form or if the responding party objects to a form that the requesting party specifies," "the responding party must state the form it intends to use for producing electronically stored information"). The reason being: "Stating the intended form before the production occurs may permit the parties to identify and seek to resolve disputes before the expense and work of the production occurs." *Id.*

Second, the manner in which mobile device data is collected can have significant implications on the format in which it can be produced. For example, when text messages are collected by taking screenshots, only a .jpg image file of the screen shot can be produced, without any message-level metadata. However, if text messages and other mobile device data are forensically collected, the data can be produced in either Excel or short-message format, depending on the collection tools used, and formats agreed, along with appropriate metadata. Because mobile device data collection is often accomplished using specialized collection software, there is real value to all parties in getting the collection process right from the outset.

These practical considerations along with the requirements established by the Rules, encourage an early and ongoing discussion of the production format of mobile device data.

A. The Variability in the Forms of Mobile device data

As discussed above, mobile devices can generate, receive, and store a wide variety of data, the existence and format of which may depend on a variety of factors, including the make and model of the mobile device and operating system, applicable software applications, location where the relevant data is stored or accessed, and end-user data retention, deletion, backup and other storage practices. Given the variability, parties and their counsel may consider whether different production formats are warranted for different custodians in a litigation matter. Therefore, counsel may be required to discuss and attempt to reach agreement on a production format that will work, given the variability in devices, data, and storage practices by individuals, custodians and corporate parties. The following are some of the currently available production formats in which parties may consider when determining the appropriate production format in which to produce mobile device data for a matter:

Short-message format: Individual text messages, mobile messaging-app messages, or other messages collected from the device combined into conversation threads (i.e., based on fixed periods of time), with attachments and embedded content included.

Individual messages: Individual text messages, mobile messaging-app messages, or other messages collected from the device and produced individually rather than grouped as conversation threads.

Mobile device screenshots: Screenshots of messages exchanged through mobile messaging applications (e.g., Signal, Telegram) not captured through traditional mobile device collection methods.

Excel spreadsheet: Text messages, contact lists, call logs and other messaging data produced in spreadsheet format.

Native file production: Production of native as-collected data complete with metadata (suitable for audio, video, PDF, word-processing documents and other files shared via text message, SMS, MMS, iMessage, or other mobile messaging applications).

As discussed in Section VI, the options available for production format may be impacted by the tools or software used to collect mobile device data. Similarly, the tools and software used to process mobile device data may affect the available production formats.

B. Factors to Consider in Assessing Appropriate Formats for Production of Mobile device data

1. Text Messages, Threads, and Metadata

One form of mobile device data that is often the subject of discovery discussions and productions is text messages. Despite the ubiquity of mobile device messaging, a clear standard has not yet emerged for how text messages should be produced in connection with litigation. Additionally, any decision or agreement on how to treat this mobile device data during the collection and search phases will have implications for the form of production. As a result, litigants currently work through these production-format questions on a case-by-case basis with limited guidance from courts.

Common issues that arise with respect to production format for text messages when working through the issues on a case-by-case basis are whether the entire conversation thread containing a responsive message or messages should be produced as a single document or whether only a single responsive message should be produced, and unitization. That is, whether the conversation thread should be broken down into unitized pieces for purposes of collection, search, review, or production, and in what increments the conversation threads should be broken down. The limited guidance from the courts on this issue suggests that if a producing party does not produce the entire conversation thread, when discussing a unitized production of text messages, the parties should consider whether unitization based on conversation day, a 24-hour period around the responsive message(s), a fixed number of messages before and after a responsive message, or some other increment (i.e., a "communication block"), is appropriate.[48]

In addressing the production format of mobile device data and unitization, courts have recognized the importance of context surrounding responsive text messages, noting that "a single text message, standing alone is oftentimes meaningless without other messages in the text chain to provide context."[49] Additionally, courts have considered whether it is appropriate to redact non-responsive

---

[48] *See* Lubrizol v. IBM Corp., No. 1:21-CV-00870-DAR, 2023 WL 3453643, at *3–4 (N.D. Ohio May 15, 2023) (observing that courts have taken different approaches to text message production format, with some suggesting that a party must produce the entirety of a text message conversation, others allowing producing parties to unilaterally withhold portions of a text message chain that are not relevant, and others taking a middle-ground approach) (collecting cases).

[49] Al Thani v. Hanke, No. 20 CIV. 4765 (JPC), 2022 WL 1684271, at *2 (S.D.N.Y. May 26, 2022); *see also* Nichols v. Noom Inc., No. 20 CV 3677L GSKHP, 2021 WL 1997542, at *3 (S.D.N.Y. May 18, 2021) (noting the reality that "it is possible that a user might have a conversation about [a relevant topic] over a period of weeks" such that the "entirety of the chat" could provide relevant context).

messages within a contextual message thread.[50] Overall, many courts have required parties to produce a limited number of unredacted and/or additional text messages or entire conversation threads to provide relevant context and preclude redactions within a contextual message thread,[51] or found that but have left it to the producing party's discretion to determine which text messages "are relevant to providing context for the other messages in the text chain."[52]

Another common issue that arises with respect to the production of text messages is what metadata can or should be produced along with the responsive messages. Again, there is little guidance from

---

50 *See* We the Protesters, Inc. v. Sinyangwe, No. 22 CIV.9565 (JPC) (GS), 2024 WL 5154077, at *6 (S.D.N.Y. Dec. 18, 2024) (held redactions within a same-day text thread were not appropriate); Harvest Church v. Resound Church, 2024 WL 5168125 (D. Colo. Dec. 19, 2024) (ordering production of redacted text messages, even though they concerned highly personal, private matters, where the nature of the relationship between the sender and recipient was at issue and could be evidenced by the personal information they shared, but limiting disclosure to attorneys eyes only and prohibiting public filing and other uses without leave of court); *Al Thani,* 2022 WL 1684271*,* at *2 (finding "no reason to go against the weight of authority in this Circuit, which holds that parties may not unilaterally redact otherwise discoverable documents for reasons other than privilege" and compelling defendant to produce unredacted chat logs because they "are relevant to providing context for the other messages in the text chain [as well as Defendants'] business dealings, and their pattern of conduct"); Vinci Brands LLC v. Coach Servs., Inc., No. 23 Civ. 5138 (LGS), Dkt. No. 347 (S.D.N.Y. Apr. 30, 2024) (following *Al Thani*); *but see* Advanced Magnesium Alloys Corp. v. Dery, No. 1:20-cv-02247, 2022 WL 3139391 (S.D. Ind. Aug. 5, 2022) (allowing producing party to redact any message or portion of a message that was purely personal in nature or related to business matters other than those at issue in the case).

51 *Id.*; *see also* S/Y Paliador, LLC v. Platypus Marine, Inc., 344 F.R.D. 110, 116 (W.D. Wash. 2023) (requiring production of text messages immediately preceding and following the produced text messages because they "could be relevant and could indicate whether the production fully encompasses the relevant conversation"); *Lubrizol*, 2023 WL 345643, at *4 (compelling production of: (1) entire message threads, where the conversation with a responsive contained 20 or fewer messages; and (2) the 10 messages preceding and following any responsive message, if the conversation contained more than 20 messages; *Al Thani*, 2022 WL 1684271, at *2 (requiring Defendant to produce unredacted chat logs because they "are relevant to providing context for the other messages in the text chain [as well as Defendants'] business dealings, and their pattern of conduct"); Sandoz, Inc. v. United Therapeutics Corp., No. 19-CV-10170, 2021 WL 2453142, at *2 (D.N.J. June 16, 2021) (ordering plaintiff to produce context-related text messages surrounding the text messages that hit search terms); BidPrime, LLC v. SmartProcure, Inc., No. 1:18-CV-478-RP, 2018 WL 6588574, at *2 (W.D. Tex. Nov. 13, 2018) (finding that "[r]ather than deeming a portion of the chat log nonresponsive and omitting it, [the defendant] should produce the full chat log."); Gipson v. Cincinnati Children's Hosp. Med. Ctr., No. 1:20-cv-294, 2021 WL 6113960, at *4–5 (S.D. Ohio Dec. 27, 2021) (ordering party to produce entirety of text message chains given court's concerns about plaintiff's self-selection of relevant messages without attorney review, noting that "[a]ll responsive messages should be produced"); Paisley Park Enters., Inc. v. Boxill, 330 F.R.D. 226, 236 (D. Minn. 2019) (ordering text messages should be provided in a manner that provides a "complete record" as opposed to "scattershot texts."); *Laub v. Horbaczewski*, 331 F.R.D. 516, 527 (C.D. Cal. 2019) (same); *but see In re* Pork Antitrust Litig., No. 18-CV-1776 (JRT/HB), 2022 WL 972401 (D. Minn. Mar. 31, 2022), at *14-15 (holding that party need only produce relevant text messages); Est. of Bailey v. City of Colorado Springs, No. 20-cv-01600, 2021 WL 2912921, at *2 (D. Colo. July 12, 2021) (holding that text messages that were unresponsive did not require any objection, redaction, or notation in a privilege log).

52 Marksman Sec. Corp. v. P.G. Sec., Inc., No. 19-62467-CIV, 2021 WL 4990442, at *2 (S.D. Fla. Mar. 19, 2021) (held that the producing party is "in the best position to determine which text message conversations require additional context and which do not, and therefore which texts require the surrounding conversation to be produced" and did not require party to produce additional text messages).

the courts, however, the guidance that exists suggests that it likely depends on the facts of the case. For example, one court held that where the document requests in question require the production of metadata, adequate responses to those requests necessarily require the production of text-message metadata.[53]

Given the lack of clear authority on this issue, it is recommended that the parties consider and reach their own agreements regarding some form of production that includes appropriate contextual messages.[54]

2. Shared Files, Attachments and Embedded Images

Mobile device data may contain audio files, videos, images, documents, or notes shared via messaging applications (e.g., Teams), and files may also be sent as attachments to individual messages. Attachments to messages may also include embedded images or emojis, in addition to the files described above. Links to websites or documents may also be sent via mobile messages. These types of mobile device data require the same considerations as files, embedded images or hyperlinks sent via email. Once a determination has been made to produce an attachment, it should be produced natively when possible and the parties should consider producing the metadata linking the documents. Including this data is often necessary for parties to determine the obligation to produce in full families or message threads, and how to define parents and attachments.

Preserving data relationships and providing context are also important considerations in determining the appropriate format for production because they can have a real impact on the merits of a case. For example, courts have held that emojis may play a pivotal role in decisions in multiple jurisdictions.[55]

---

53 Witham v. Hershey Co., No. 23-CV-1563 (LMP/JFD), 2025 WL 444399, at *4 (D. Minn. Feb. 10, 2025) (held plaintiffs' "screenshots of the messages he thought were responsive" was "a hopelessly inadequate way to search for and produce documents responsive to an RFP in federal court").

54 *We the Protesters, Inc.*, 2024 WL 5154077, at *3 ("Litigants are free to—and are well-advised to—mitigate the risk of this uncertain legal regime by coming to their own agreement about how to address text messages in discovery.").

55 *In re* Bed Bath & Beyond Corp. Sec. Litig., No. 1:22-cv-2541 (TNM), 2023 U.S. Dist. LEXIS 129613 (D.D.C. July 27, 2023) (denying motion to dismiss securities fraud suit predicated upon defendant's tweet of a moon face emoji that his followers interpreted signaling that the stock would go "to the moon," reasoning that the "symbol's meaning may be clarified by 'the context in which [it] is used" including mime "subculture" and noting that relevant responses provided additional relevant context) (citation omitted); State v. D.R.C., 467 P.3d 994, 1001 (Wash. Ct. App. 2020)(admitting emoji in evidence and noting tone associated with an anthropomorphic emoji can materially alter the meaning of surrounding text when an emoji conveys facetiousness)); Ghanam v. Does, 845 N.W.2d 128, 145 (Mich. Ct. App. 2014) (same); and Crawford v. Mangos Caribbean Rest., LLC, No. 1:18-CV-4450-JPB-JCF, 2020 WL 10056405, at *5 (N.D. Ga. July 30, 2020), *report and recommendation adopted*, No. 1:18-CV-4450-JPB, 2020 WL 10056404 (N.D. Ga. Sept. 2, 2020) (holding a "peace sign has been offered as evidence of quitting a job).

IX. IMPACT OF INFORMATION GOVERNANCE CONSIDERATIONS ON MOBILE DEVICE DATA

From its position on the far left of the EDRM process, information governance, if adhered to, can have a significant positive impact on the discovery of mobile device data. Guidance on appropriate considerations for policy drafters and program designers exists in abundance.[56] This paper does not purport to update or supplant that guidance. However, understanding the essential elements of an effective information-governance program, and how such a program addresses mobile device data, is essential to developing an effective approach to offensive and defensive discovery.

The ubiquitous presence of mobile devices in today's world, along with the ephemeral nature of some data that only exists locally on those devices, creates an obligation for companies to be strategic in their approach to all categories of mobile device data.

Information-governance programs should address mobile device data and should consider the equipment, nature of use, and communication practices with respect to mobile devices that are part of a party's mobile ecosystem. Essential elements of a comprehensive program include a mobile device framework (e.g., BYOD, COPE, COBO) that:

Is consistently applied, monitored, and enforced with respect to all employees who use or access corporate data from mobile devices, with minimal departures/exceptions from that framework.[57]

Considers preservation, collection, and discoverability needs with respect to mobile device data, adopts framework for preserving, collecting and discovering mobile device data in a mobile device policy, and mandates employee training to promote compliance and provide education on acceptable use of mobile devices in accordance with such policies.[58]

As discussed below and elsewhere in this *Commentary*, given fact-specific holdings in mobile device discovery litigation, organizations must consider whether they have the legal right or practical ability to control a mobile device and be transparent to opposing counsel so preservation letters and/or

---

56 *See, e.g., Using the IGRM Model*, ECRM, https://edrm.net/resources/frameworks-and-standards/information-governance-reference-model/using-the-igrm-model/ (last visited Mar. 25, 2025); RESOURCES.DATA.GOV, https://resources.data.gov/ (last visited Mar. 25, 2025); INFORMATION GOVERNANCE IMPLEMENTATION MODEL (IGIM) (ASSOCIATION OF RECORDS MANAGERS AND ADMINISTRATORS 2022) (available at https://www.path-lms.com/arma-international/courses/60736.

57 *See, e.g.*, Magdalena Martens-Patynska, *BYOD, CYOD, COPE, COBO, COSU – explore mobility management strategies,* PROGET, Jan. 16, 2023 https://proget.pl/en/blog/byod-cyod-cope-cobo-cosu/ (BYOD: "Bring Your Own Device"; CYOD: "Choose Your Own Device"; COPE: "Company Owned/Personally Enabled"; COBO: "Company Owned/Business Only"; COSU: "Company Owned/Single Use").

58 *See Commentary on BYOD, supra* note 5, comment 2.c.

Rule 45 third-party subpoenas can be served to preserve and collect relevant data if the company determines it does not have "possession, custody or control".[59]

Directs employees to limit business communications/collaboration to approved mobile devices and applications/platforms that synchronize data with enterprise-accessible tools. But, of course, the company may not be able to limit such communications, and to the extent a company prefers a bring-your-own-device policy, they should understand that there will be a need to monitor and enforce the policy, and if litigation ensues, there will be collections from third parties.

Considers MDM and mobile device data archiving tools to (i) enforce compliance with the mobile device framework; (ii) maintain an inventory of devices and installed applications; and (iii) facilitate data preservation and collection obligations.

Includes employee onboarding procedures that expressly address the legal and data security and privacy implications of using mobile devices to conduct or communicate about business-related matters, including regarding:

Requires advance authorization to access corporate information on personal devices.

Addresses and accounts for the potential need to collect or retain access to mobile devices' data from departing employees.

Evaluates the impact of mobile-data security on preservation/collection obligations.

Corporate litigants and targets of governmental investigations risk possible spoliation allegations if their corporate policies and programs regarding mobile device data fail to adequately incorporate and adhere to these elements. For instance, the court in *Miramontes v. Peraton* imposed sanctions on the defendant employer, holding that the defendant had control over relevant text messages that the plaintiff employee's former supervisor deleted from his personal phone. The court considered these four factors:

Whether the employer issued the devices;

How frequently the devices were used for business purposes;[60]

Whether the employer had a legal right to obtain communications from the devices; and

---

[59] *In re* Pork Antitrust Litig., No. 18-CV-1776 (JRT/HB), 2022 WL 972401 (D. Minn. Mar. 31, 2022), at *4 (the Eighth Circuit has never decided whether the "legal right" or "practical ability" standard should govern, and other circuits are split on the issue, citing *See Commentary on Rule 34 and Rule 45, supra* note 15 at 467, 482–92.

[60] *Supra* note 3.

Whether company policies address access to communications on personal devices.[61]

In finding the requisite control, the court emphasized the second factor as the overriding consideration, not wanting to give corporate litigants a path to shield communications from discovery when employee use of personal devices for business purposes is pervasive, even if not formally endorsed.

By contrast, in *Rattie v. Balfour Beatty Infrastructure, Inc.*[62] the plaintiff failed to establish that the defendant had possession, custody, or control over relevant text messages on its employees' personal phones, finding persuasive defendant's "represent[ation] to the Court that it issues work phones to its management employees, and that they are expected to use these devices for work-related communications."[63]

Given the fact-specific nature of judicial opinions regarding preservation and discoverability of mobile device data, the best guidance for corporate entities may be to practice what they preach: If corporate policy prohibits employees from using personal devices for business purposes, the corporate entity should take steps to monitor and enforce that policy. If, conversely, the employees are authorized to use personal devices for business purposes, assume relevant communications on those devices will be discoverable and act accordingly.

Likewise, the DOJ, in March 2023, issued a revised Evaluation of Corporate Compliance Programs (ECCP) policy with a clear focus on communications data.[64] As part of the revised ECCP, the DOJ provides guidance on how it will assess corporations' policies and procedures around the use of company devices, messaging applications, and other communications platforms in the workplace. The ECCP sets forth detailed questions that prosecutors should ask when evaluating a company's policies. For example, prosecutors are now directed to determine whether a corporation's policy allows the company to review business communications on personal devices and messaging applications and whether employees are required to transfer messages from messaging applications to company recordkeeping systems to preserve and retain them.[65] Similarly, prosecutors will be tasked with evaluating whether there are consequences for employees who refuse to provide access to business

---

61 Miramontes v. Peraton, Inc., No. 3:21-CV-3019-B, 2023 WL 3855603 (N.D. Tex. June 6, 2023).

62 2023 WL 5507174 (N.D. Cal. Aug. 25, 2023)

63 Rattie v. Balfour Beatty Infrastructure, Inc., No. 22-cv-05061-RS (LJC), 2023 WL 5507174 (N.D. Cal. Aug. 25, 2023).

64 U.S. Dept. of Justice Criminal Division, Evaluation of Corporate Compliance Programs (updated Sept. 2024), *available at* https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl). *See also* FTC and DOJ Update Guidance That Reinforces Parties' Preservation Obligations for Collaboration Tools and Ephemeral Messaging (Federal Trade Commission Jan. 26, 2024) (available at https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-doj-update-guidance-reinforces-parties-preservation-obligations-collaboration-tools-ephemeral).

65 *See, e.g., Further Revisions to Corporate Criminal Enforcement Policies Following Discussions with Corporate Crime Advisory Group* p. 11 (U.S. Department of Justice Office of the Deputy Attorney General Sept. 15, 2022) (available at https://www.justice.gov/d9/pages/attachments/2022/09/15/2022.09.15_ccag_memo.pdf) (referencing "Use of Personal Devices and Third-Party Applications").

data on personal devices and whether any employees have been disciplined for not providing such access. They are to scrutinize the company's "policies and procedures governing the use of personal devices, communication platforms, and messaging applications" closely.[66] These policies should be "tailored to the corporation's risk profile and specific business needs" and ensure that business-related communications are accessible and preserved "to the greatest extent possible."[67]

66 *Supra* note 6 at 1.

67 *Id.*