

Draft Commentary on Discovery of Mobile Device Data

The Sedona Conference

April 2024

Copyright 2024. All rights reserved.



This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

Draft Commentary on Discovery of Mobile Device Data

Sedona Conference Working Group 1

[Draft 04/12/2024]

Drafting Team Members

Alicia Clausen
Rachel Kaufman
Jason Lichter
John Pappas
Lars Schou
Deric Yoakley

Shauna Itri
Warren Kruse
Margaret Malloy
Robin Perkins
Daniel Stromberg

Team Leaders

Dennis Kiker

Michelle Newcomer

Steering Committee Liaisons

Robert Keeling
Maria Salacuse

Daniel Lim

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

I. INTRODUCTION

The use of mobile devices has become ubiquitous. As a result, it is not surprising that they have become an increasingly relevant data source in litigation. The discovery of mobile device data raises unique issues that must be considered when identifying, preserving, collecting, processing, searching, reviewing, and producing this type of data. However, case law on mobile device discovery is often case specific and may not provide parties and practitioners with a clear legal framework necessary to confidently meet their discovery obligations related to mobile devices.

This Commentary is intended to be both legal and practical in orientation and provide guidance to parties, counsel, and the courts on relevant standards and factors impacting discovery of mobile device data, while addressing evolving technical issues affecting these data sources. It also will provide guidance for preserving, collecting, processing, searching, reviewing, and producing mobile device data.

II. WHAT IS A MOBILE DEVICE AND WHAT DATA IS STORED ON OR ACCESSIBLE FROM A MOBILE DEVICE?

There is no single, universally accepted definition of *mobile device*. Many courts have resolved disputes concerning mobile device discovery,¹ but there are few, if any, published decisions expressly defining the term and what it does (and does not) encompass. Perhaps in response to the dearth of judicial guidance, some parties have elected to define what they consider a mobile device in electronic discovery protocols that courts have subsequently entered. For instance, in *In Loomis Sayles Trust Co., LLC v. Citigroup Global Markets Inc.*, the court entered an ESI protocol that defined “Mobile Device” as “any mobile phone, cellular phone, or tablet device (e.g., iPhone, iPad, Android-compatible devices, or Microsoft Surface Go)”.² But definitions of this sort are problematic in their wholesale reliance on specific make/model examples³ rather than universal criteria that can be applied to new types of devices.

The National Institute of Standards and Technology (“NIST”) has issued no fewer than nine (9) distinct mobile device definitions across its many publications.⁴ This Commentary adopts the following baseline definition of mobile device from NIST Special Publication 800-79-2 but refines it with three supplemental prerequisites added below.

¹ 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.*, 2023 WL 3855603 (N.D. Tex. 2023); *Laub v. Horbaczewski*, 331 F.R.D. 516, 527 (C.D. Cal. 2019).

² *Loomis Sayles Trust Co., LLC v. Citigroup Global Markets Inc.*, No. 1:22-cv-06706-LGS (S.D.N.Y. Jan. 24, 2023).

³ While it may literally be a device that is mobile, the parties’ characterization of Microsoft’s Surface Go tablet as a mobile device would be at odds with this Commentary’s guidance that devices running operating systems generally associated with desktop and laptop computers (here, Windows) for which other Sedona guidance is more directly applicable should not be conflated with true mobile devices.

⁴ These definitions are aggregated in NIST’s *Computer Security Research Center Glossary*, available at https://csrc.nist.gov/glossary/term/mobile_device.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

A mobile device, for the purpose of this document 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, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include 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.

While each of the four attributes set forth in the above NIST definition is a necessary condition to qualify as a mobile device, there are three additional limiting elements for purposes of this Commentary:

1. Pure Internet of Things (“IoT”) devices (e.g., smart home assistants/hubs) are excluded;⁵
2. The primary purpose of the device must be for *communication or content creation*; and
3. 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 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 it may still be instructive).

Many other devices would fall outside the scope of this Commentary but could still contain information requiring preservation, collection, processing, search, review, and production. For instance, a small GPS tracker could contain discoverable information regarding someone’s whereabouts, and a voice recorder could contain highly relevant audio recordings. The balance of this Commentary, however, will delve into the unique challenges associated with discovery from mobile devices as that term has been circumscribed in this section.

Mobile device data is data that is stored on or accessible from the device itself. Examples of mobile device data that is stored on a mobile device typically include text messages (i.e., SMS/MMS messages), voice messages, call logs/histories, contacts, calendar entries, appointments and reminders, location data (e.g., GPS coordinates and location history), photographs, videos, notes, locally stored passwords, internet browsing history, documents; applications that store messages, files, and other data locally. Mobile device data may also include 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 in the Cloud). However, the mobile device may not be considered to be the primary source of such data for discovery purposes. These are only current examples and mobile devices and related systems and applications are

⁵ [INSERT CROSS REFERENCE TO SEDONA’S PENDING IoT PUBLICATION]

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

constantly evolving. Accordingly, insofar as this paper provides guidance with respect to discovery of mobile devices and mobile device data, it does so 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 and proportional to the needs of the case. 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. Mobile devices and mobile device data need not be admissible in evidence to be within the scope of discovery.

Accordingly, 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 may consider 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. 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 (v) whether the relevant data is accessible from multiple sources (e.g., cloud accounts or other storage), and which source is more reasonably accessible. However, every situation should be assessed on its own terms, and the fact that particular mobile device data might be accessible from another source does not mean that the mobile device is immune from discovery, including preservation requirements.⁶

Where an organization is involved, consideration should also be given to whether and the extent to which mobile devices were utilized within an organization to communicate about or conduct business and the extent to which the mobile device data stored on or accessible from those devices, are within the organization's possession, custody or control.⁷ Questions that may inform this inquiry include:

- Whether the individuals whose devices may be at issue are current or former employees, a named party, or otherwise receiving payment from the organization?⁸

⁶ FED. R. CIV. P. 26(b)(1), 26(b)(2)(B); 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).

⁷ Guidance for 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," and will not be discussed further herein. See The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," 25 SEDONA CONF. J. 1 (forthcoming 2024).

⁸ The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," 25 SEDONA CONF. J. 1 (forthcoming 2024); *Chevron Corp. v. Salazar*, 275 F.R.D. 437, 448-49 (S.D.N.Y. 2011) ("[c]ourts have repeatedly found that employers have control over their employees and can be

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

- Whether the individuals who possess or control the data are officers, Board members, or other agents of the organization?⁹
- Whether the individuals have or had a fiduciary relationship with the organization;¹⁰
- Whether the records sought from the individual's mobile device are the type of records that the organization would be likely to have access to, or request in the normal course of business;¹¹
- Whether there is an employment contract, severance agreement, or any other agreement or document that requires the individual to provide materials or otherwise cooperate with company investigations or litigation;¹²
- Whether there are other company policies that require the individual to cooperate with company investigations or litigation;

required to produce documents in their employees' possession"); *Canton v. Hoaglin*, 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").

⁹ 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 *In Riddell Sports Inc. v. Brooks*, 158 F.R.D. 555, 558 (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. Maritime 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).

¹⁰ *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"))).

¹¹ *In re Pork Antitrust Litig.*, No. 18-CV-1776 (JRT/HB), 2022 WL 972401, at *7 (D. Minn. Mar. 31, 2022) (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).

¹² See, e.g., *Flagg v. City of Detroit*, 252 F.R.D. 346, 353–54 (E.D. Mich. 2008) ("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)).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to

comments@sedonaconference.org

- 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;¹³
- Whether the party asked the individual for the mobile device or access to the mobile device data;¹⁴
- Whether the data is stored on an organization-issued or owned device;
- What the organization's policies or procedures 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;
- Whether the organization knowingly lets employees use their personal devices;¹⁵
- Whether the organization utilizes any other tools to monitor or access data on an employee's mobile devices.

BYOD policies may also inform the extent to which an organization may have control over or access to an employee's mobile devices. BYOD policies will necessarily vary from organization to organization, but consideration should be given to whether a BYOD policy: (i) explicitly requires

¹³ See, e.g., *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 as a factor non-party's past history of cooperating with document requests" (citing *Alexander Interactive, Inc. v. Adorama, Inc.*, 2014 WL 61472, at *3 (S.D.N.Y. Jan. 6, 2014)); see also *In re Pork Antitrust Litig.*, No. 18-CV-1776 (JRT/HB), 2022 WL 972401, at *3–4 (D. Minn. Mar. 31, 2022) (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. 493, 530–31 (S.D.N.Y. 1996) (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).

¹⁴ See, e.g., *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); *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.*, 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").

¹⁵ *Miramontes v. Peraton, Inc.*, 2023 WL 3855603 (N.D. Tex. 2023).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

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 utilize 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) explicitly 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.

The extent to which organizations utilize mobile device management tools to monitor, back-up, or archive data on mobile devices used by its employees may also inform whether it has access to or control over an employee's mobile device data, as well as its ability and obligation to preserve and produce such data in litigation. On the other hand, even where mobile device data associated with Mobile Device Management (MDM) tools, archives or cloud backup is accessible by the organization, it may become more readily accessible from the mobile device if the primary source becomes unavailable.¹⁶

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 your matter.¹⁷

IV. GUIDANCE FOR IDENTIFYING RELEVANT MOBILE DEVICE DATA SOURCES.

Identifying mobile device data that may be subject to discovery is an important threshold task. Parties should seek to identify all individuals who may have relevant information on their mobile devices, and all of their mobile devices that may have relevant information. Parties and their counsel may 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.

Written questionnaires may be a useful tool to collect preliminary information regarding the potential mobile devices and mobile device data at issue. However, 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 may also 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 device data that may contain discoverable information where the relevant devices and data are located,

¹⁶ For more information the applicable standards governing the determination of a party's possession, custody or control over discovery, see *The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467 (2016); *The Sedona Conference Commentary on BYOD: Principles and Guidance for Developing Policies and meeting Discovery Obligations,* 19 SEDONA CONF. J. 495 (2018); *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production,* 19 SEDONA CONF. J. 1 (2018).

¹⁷ THE SEDONA COOPERATION PROCLAMATION (2008).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

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, and production of relevant data from those devices.

Among other things, for individual litigants, parties should endeavor to learn:

1. What types of mobile devices the individual utilized during the relevant time period;
2. What relevant data and communications each device may contain (e.g., emails, text messages, documents);
3. How the individual stored or accessed that data on the mobile device;
4. What applications or communications tools installed on the devices were used to store or communicate the relevant information;
5. Was data ever transferred from one device to another;
6. Whether the party still has the mobile device(s) in question, and if not:
 - a. What happened to the device(s);
 - b. When; and
 - c. Was any data transferred to a new device or backed-up prior to its loss/disposition
7. Any security methods or encryption utilized on the device;
8. If applicable to the legal matter, whether location services or other features that track location or movements are or were enabled;
9. The make and model of the devices, the operating system installed, and the service provider;
10. How mobile device data is stored (e.g., locally v. cloud, etc.);
11. 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;
12. How the individual typically handles data preservation, including whether s/he regularly backs-up data from the mobile device(s), how often, and where; and
13. 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.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

Additionally, where a corporate party is involved, counsel should endeavor to learn:

1. Whether employees utilized mobile devices to communicate about or conduct business during the relevant period;
2. Whether any software applications or communication tools installed on those devices were used to communicate about or conduct business and/or communicate about the claims or defenses in the litigation;
3. Which employees utilized such mobile devices;
4. Whether the employees are current or former employees;
5. Whether the mobile devices used were company-issued or personal devices;
6. Whether the company is in possession of the devices at issue;
7. 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 to communicate about or conduct business;
8. Whether mobile device management tools or container software were utilized on the mobile device; and
9. Whether any back-up systems or procedures were in place to back-up or archive data on the mobile device.

Sampling can also be used to help identify and assess whether discoverable mobile device data may be subject to discovery.

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. These obligations generally extend to all such data within a party’s possession, custody or control. To the extent a party deems relevant mobile device data to be outside of its possession, custody, or control, it may consider issuing preservation subpoenas to the persons or entities who are in possession, custody or control of those devices or data to ensure their proper preservation.

Additionally, Rule 26(f) of the Federal Rules of Civil Procedure require parties, at the outset of a matter, to discuss the preservation, disclosure, and discovery of ESI during this conference, 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 that 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 ensuring that all potentially relevant information is considered and addressed early in the litigation. Among other things, it allows parties to understand the potential sources of relevant

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

documents and information in the case, and actions they may need to take to obtain or ensure the 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 electronically stored information and requires a party to make reasonable and good faith efforts to retain discoverable information.¹⁸ A party's preservation obligations and efforts are assessed on a case-by-case basis and must be reasonable under the circumstances.¹⁹

In evaluating what preservation steps are reasonable with respect to a particular mobile device, the inquiry should begin with an investigation into the scope of discoverable information on 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.²⁰ 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 are clarified during the pendency of a matter."²¹

Preservation decisions should be guided by a fact-based understanding of the sources and types of discoverable data on the device, as well as the location and accessibility of the devices and data in question. Additional considerations may include the likely volume of discoverable data, the

¹⁸ *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 93 (2018); The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341, 385 (2019).

¹⁹ *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 67 (2018); The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341, 354-55 (2019).

²⁰ *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 101-02 (2018); The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341, 357 (2019).

²¹ *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 96 (2018).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

uniqueness, and available techniques for preservation along with associated costs and burdens.²² It is not necessary for a party to preserve multiple or duplicative copies of mobile device data, and “even the sole copy of an ESI item need not be preserved if doing so would be disproportionate to the needs of the case.”²³

A. Preservation Methodologies.

Mobile device preservation methods exist on a continuum and can vary greatly in terms of effectiveness and cost. For example, depending on the circumstances, a party may be able to meet its preservation obligations by sending a well-drafted legal hold notice to the custodian 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 the data could be lost in any number of ways such as the custodian failing to follow the legal hold instructions, losing the device, breaking or damaging the device, exchanging the device for a different model without taking necessary steps to back-up or transfer the relevant data, performing a factory reset of the device, or deliberately deleting content.

At the other end of the preservation continuum, the party may need to 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, method of collection, available tools, and party involved. In addition to the monetary expense, scheduling and coordinating a collection process involving the vendor, 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 data to an external location (e.g., cloud repository, server, drive, or other location), 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. Additional factors to consider in determining appropriate preservation methods include 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 because of automated processes designed to manage the limited memory space available on the device or through inadvertent actions by the user.

Ultimately, parties may weigh the costs and benefits of each option in determining which method is appropriate to meet its preservation obligations for the matter.²⁴ A party must also be mindful that its preservation obligations, including the appropriate preservation method, may be

²² The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 Sedona Conf. J. 341, 389-98 (2019).

²³ *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 94-96 (2018).

²⁴ *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 63 (2018).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

subject to change, for example, as the matter progresses and more information becomes known or discovery requests are served, among other things.

1. Technical Proficiency of the Possessor/User.

By their nature, mobile devices are often in the possession of individuals that lack legal and technical sophistication, which is a factor that parties, counsel, and courts may consider when evaluating the reasonableness of preservation efforts, particularly with individual litigants. Sophisticated parties are often held to a higher standard for preservation of mobile devices and mobile device data. Counsel should evaluate their client's level of sophistication when providing guidance on the appropriate steps for mobile device data preservation. With less sophisticated parties, counsel may also consider whether it is preferable to collect mobile device data proactively to avoid potential spoliation issues. However, even when the mobile device is "managed" by a sophisticated IT department, there may be relevant information that is unmanaged, such as location data or other information that uniquely resides on the mobile device.

2. Where Preserved Data Will Reside.

When developing a preservation plan, thought must be given as to where the preserved data will reside. In some instances, data may be preserved "in place," (i.e., on the device) by turning off the auto-delete setting on the device itself. If available, preservation can be managed by use of MDM software, by limiting the individual's access to data managed by the MDM on the device. Another preservation option is having the mobile device back-up to its associated cloud storage repository (e.g., Apple's iCloud, Samsung Cloud, etc.). If forensically collected, the data will typically be stored by counsel or a vendor in a secure location. With any of these options, steps must be taken to ensure the preserved data is secure and cannot be manipulated or deleted.

However, there may be instances where mobile device data must be collected and preserved locally. In those instances, the data must be preserved in a way that reasonably ensures that it is not lost, that it will not be tampered with, and that the mobile device owner's data will remain private.

B. Cooperation and Transparency: Managing Expectations

As will be discussed in Section 6, *supra*, mobile device data is very different than the electronically stored information that parties have traditionally preserved and produced and presents unique challenges for preservation. Among other things, mobile device data is volatile and ever-changing while the device is powered-on, unlike traditional computing devices, and network shares, and most mobile device operating systems store data in database form, unlike non-mobile devices. Accordingly, in the context of mobile device data discovery, some level of transparency into the methodologies and technologies at the preservation stage may be in the best interests of a specific case. In a matter where both the requesting and the receiving parties are sophisticated and well-versed in the intricacies of mobile device data discovery, little or no discussion may need to occur regarding methodologies and technologies the parties will utilize in preserving and producing their own mobile device data discovery.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

In other cases, some level of transparency into methodologies and technologies early in the process may be necessary to manage the expectations (and possibly foment some cooperation) of the requesting party. For a further discussion of the different challenges mobile device data presents, see Section 6, *supra*.

In sum, because mobile device data presents a different challenge, involving the requesting party at the preservation stage might help lessen the burden on the preserving party at the collection, review, and production stages.

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

The choice of mobile data collection method depends on various factors, including the nature of the matter, the type of applications used, and the way the custodian uses their mobile device. No two custodians may use a mobile device the same way. In the realm of digital forensics, the methods of collection are crucial for gathering data effectively while ensuring its integrity and admissibility in legal proceedings. The process of collecting mobile evidence involves various techniques tailored to the specific devices and applications involved. Prior to collection custodial interviews and IT interviews would offer unique insights into the usage patterns and content present on mobile devices.

A. Custodial Interviews

Custodial interviews play an important role in determining the appropriate collection method for the matter. In conducting a custodial interview, it is crucial to gain information about how the device is or was utilized, including details about applications, communication channels, and data storage practices, including:

- **Insights into Application Usage:** By interviewing custodians, forensic experts and counsel can gather information about the applications installed on the device, including messaging apps, social media platforms, and productivity tools. This knowledge helps prioritize data collection efforts.
- **Understanding Communication Patterns:** Custodial interviews provide valuable insights into how the device is used for communications potentially related to the matter, such as the frequency of messages, contacts, and preferred communication channels.
- **Identification of Data Storage Locations:** Custodians can provide information about where specific types of data are stored on the device or in the cloud, aiding in targeted data collection. Custodians can identify others that may have been participants or recipients on communications. Once collected, analysis of the data may identify other people communicating that should be considered for unique mobile content.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

B. Manual Collection for Encrypted Apps

Messages sent through encrypted applications like Signal may require manual collection efforts since the data is not readily accessible through conventional means. Encrypted message may be collected, but the encryption will make them unusable. Manual collection via screen shots or other methods may be the only means available for collection.

C. Targeted Manual Collection with Party Agreement

Targeted collections may also be suitable in certain situations where the metadata will not be at issue. In such cases, screen shots or individual files collected manually may be sufficient. Such collections should only be used where the parties are in agreement about the approach as the lack of original metadata could adversely impact the ability to authenticate the documents collected.

D. Physical Acquisition in Criminal Investigations

In criminal investigations, law enforcement agencies may opt for physical acquisition of the device, followed by jailbreaking or rooting procedures to access restricted data. In civil matters, there are currently two solutions for a full collection that allow access to a locked device:

- GRAYKEY
- Cellebrite Premium

These are currently available to law enforcement and non-law enforcement. Physically possessing the device is currently required since both have a physical device the mobile needs to be connected to, so remote collection is not currently an option.²⁵

E. Logical Collections in Civil Proceedings

In civil proceedings, collections often involve logical extraction methods that do not require physical possession of the device, ensuring minimal disruption to the device owner's use of the device.²⁶

In cases where data is exclusively available on the device and cannot be obtained from remote servers, collection from the mobile device becomes essential. This method ensures that pertinent

²⁵ “Remote collection” refers to a collection performed where the physical device is not in the possession of the person collecting the data and is typically performed over the Internet.

²⁶ 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). Logical extraction cannot recover deleted files or be used on a locked device. Logical extraction also does not include a bit-by-bit copy of the mobile device.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

evidence is gathered directly from the source, maintaining its integrity and admissibility in legal proceedings.²⁷

Other data accessible from the device, such as email and certain messaging applications, such as Slack or Microsoft Teams, is typically stored on external servers, or in cloud repositories, and can more easily be collected from those sources without obtaining the device itself. However, there are instances where collecting messages from a mobile device becomes necessary:

- **Inaccessible Server:** If the server hosting the messages is inaccessible due to technical issues or legal constraints, collecting messages directly from the mobile device may be the only viable option. Depending on the configuration of the email application being used, the type of device and the device operating system, full emails may not be available for collection. Email is typically not able to be collected on modern devices without collecting a full file system using appropriate forensic software.
- **Cached Messages or offline usage:** Certain messages may be cached on the mobile device, making them available locally even if they are not stored on the server. In such cases, mobile collection ensures the retrieval of these messages for forensic analysis.

By collecting data directly from the mobile device investigators, parties and counsel, can access data that may not otherwise be available through remote servers, ensuring a more comprehensive examination of digital evidence. Additionally, forensic examiners can preserve evidence in its original state, minimizing the risk of alteration or tampering. Since a mobile device is always changing when it is on, preserving as soon as possible may be advisable.

Forensic collection of a mobile device can be conducted through different approaches:

- **Full File System:** This method involves creating a complete forensic preservation the mobile device's storage, capturing all accessible data, including, application data, and deleted content.
- **Logical extraction:** Alternatively, counsel may opt for a logical extraction, rather than capturing the full file system.²⁸
- **Comprehensive Data Extraction Tools:** Tools such as Cellebrite Premium or GRAYKEY offer advanced capabilities for extracting detailed data from iOS and modern Android devices. These tools provide access to a wide range of data types,

²⁷ For example, WhatsApp, a popular messaging application, typically stores messages on its cloud servers for up to 12 months. However, additional messages beyond this timeframe may be stored locally on the mobile device. Therefore, in situations where historical messages are required beyond what is available on the cloud, mobile collection becomes necessary to access the complete set of data.

²⁸ See note 26, *supra*.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

including deleted data, pictures, videos, chat histories, location data, and Internet evidence.

Full device imaging allows for a deeper collection of data, providing forensic examiners with a comprehensive view of the device's contents. This method ensures that no potentially relevant evidence is missed during the investigation process. By capturing a complete forensic image of the device, examiners can access deleted data that may be crucial to the investigation. In most cases, logical collection is appropriate and proportionate. Full device imaging is most often warranted where deleted or fragmented data are potentially relevant.

Post collection, a report on the device's installed applications, currently installed on the device, should be reviewed to potentially identify other applications, previously not known, that may be pertinent to the matter.

F. Privacy Considerations for Mobile Collections

Depending on the circumstances, parties may consider certain privacy interests an individual may have in non-relevant data on their mobile device, in determining the appropriate method of collection. For example, a targeted collection can address custodian privacy concerns by focusing only on specific data categories or folders. This approach may be preferred in cases where privacy considerations are paramount.

Collections performed in countries with strict privacy laws (e.g. the EU's GDPR or China's DSL) may raise additional concerns. This may raise obstacles to the collection of the data or require the collection to be performed and the relevant data identified before any data is transferred to another jurisdiction. There may also be restrictions on the use of the data after it is collected.

In summary, the methods of collection for mobile evidence encompass a combination of custodial interviews and device collection methods, each offering valuable insights 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.

Mobile devices have become repositories for a vast amount of potentially relevant information in legal investigations. Effectively searching this data requires careful consideration of various factors to ensure a thorough and defensible approach.

A. Factors Influencing Search Methods

1. Initial Investigation and Data Assessment.

To develop an effective and defensible search methodology, it is crucial to conduct an initial investigation including custodial interviews and data assessment. Information is needed about the data

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

sources on the mobile device that are 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. For communications, it is essential to identify the participants involved and the messaging frequency. Another important piece of information is whether any potentially discoverable data is encrypted. Encrypted data can significantly impede search and extraction capabilities. It is generally not searchable and will not be included in search results. It may be necessary to explore potential legal avenues to access encrypted data in investigations with proper authorization, while recognizing the importance of upholding user privacy rights and data security best practices.

Custodial interviews are an important way to gather information when developing a search methodology. Custodians should be asked about the types of potentially discoverable data sources on the mobile device, the use of specific terms or abbreviations, communication/chat participants, relevant time periods, and the use of third-party applications. Information obtained during custodial interviews may be used to guide the scope of the search, but verification measures may be warranted. Interviews of IT personnel should also be conducted to determine data storage practices (e.g., cloud backups) and retention policies.

Sampling can be used to aid in development of a search methodology. In some instances, sampling a representative subset of the mobile device data subject to search might be helpful in identifying potentially discoverable data sources, developing appropriate search criteria, assessing the efficacy of searches, and verifying information provided by custodians. Sampling may include a subset of custodians, a subset of time periods or a subset of search terms.

Utilizing data assessment and visualization tools can also aid in the development of effective searches. These tools enable exploration of communication patterns and identification of potential anomalies. For example, creating network graphs can reveal key players within a communication network, visualizing who communicated most frequently with whom. Timeline visualizations can showcase the flow of communication over time, potentially highlighting periods of increased communication activity.

2. Collection Methods.

The means by which mobile device data is collected significantly impacts available search options. Methods range from manual collection of screenshots and individual files to forensic extraction of all accessible data 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. This type of collection can be searched in many different ways including searches of both data content and associated metadata. On the other hand, if the collection consists only of screenshots or video captures, searching capabilities will be quite limited.

3. Data Type and Tool Considerations.

To develop an appropriate search methodology, it is important to consider the type of data being searched. For instance, searches based on participants and date ranges are generally more effective for chats than keyword searches. In chats, participants tend to speak more informally, using

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

emojis and abbreviations, making typos, and sending messages with erroneously auto-corrected text. 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. With these types of data, relying solely on strict keyword searches can be ineffective and not reasonable or defensible. For instance, searching for "meeting" might miss messages or notes referring to a "mtg" or "meetup." Using a "fuzzy match" search may help to mitigate this issue because it allows for variations in spelling, accounting for typos and user-generated abbreviations commonly found in mobile communications.

In evaluating the potential use of keyword searches for searching mobile device data such as messages or chats, there are additional factors to consider. The manner in which chats are processed and viewed can also impact the usefulness of search terms. 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.

The tool being used can also impact the effectiveness of the search methodology. For instance, many industry-standard mobile forensic tools lack support for advanced search operators like wildcards (*) or proximity searching (terms appearing within a specific number of words from each other). To run complex searches, it may be necessary to export the collected data from the forensic tool into an attorney review tool with more robust search capabilities. Similarly, some forensic tools might not support transcription of media files like voicemails, audio recordings, or videos, and this data must be loaded into a different review tool before running keyword searches.

4. Advanced Analytical Tools.

The use of advanced analytics tools, such as machine learning, predictive coding, or other artificial intelligence-based tools, may be considered as part of a search methodology, but there are a number of reasons why AI tools might not work well with mobile data. First, mobile data may be incomplete, contain informal dialogue, abbreviations, acronyms, emojis, slang, and autocorrections that may not be suitable for advanced analytic tools, which often are premised on algorithms that analyze text. Second, the amount of mobile device data available to train AI models may be smaller compared to other domains, hindering accuracy. Third, understanding how AI tools utilized reach their conclusions will be important in determining whether a party has satisfied its obligations to conduct a reasonable search. AI may be more useful as an analytical tool after conversation threads have been created (e.g., in short message format), after the data has been collected.

Other advanced analytic tools may be more effective with mobile device data such as regular expression searches. These tools enable searching for specific patterns within the data, like phone numbers (e.g., a regular expression can capture variations in phone number formats across different countries). They can also be used to identify email addresses or specific keywords phrased in a particular way.

Another useful tool is textual near duplicate analysis, which can help identify messages with similar content. Leveraging this tool is particularly beneficial on data sets that are not amenable to standard, hash-based deduplication including some types of chats.

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

5. Cooperation/Transparency Related to Search Methodology.

In developing an appropriate search protocol for mobile device data, the responding 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.²⁹ However, it can be beneficial for parties to disclose and discuss the search methodology to be applied early in the discovery process. This can aid in the development of effective searches and prevent disputes and misunderstandings that may result in collateral litigation. Depending on the jurisdiction, such disclosures may be required by applicable court rules.³⁰ It may also be appropriate, or even necessary, to disclose information about sampling methodologies that were utilized for identification, searching, and validation.

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 an appropriate format or formats 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 format or formats for the production of mobile device data.

While production format is normally considered one of the last steps 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 form 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 must have a comprehensive understanding of what relevant mobile device data may be within their clients’ possession, custody, and control 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 all parties will benefit from accelerating an investigation of these issues to inform a discussion about how the parties will practically address these issues. One way to do so is to address and reach 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. See Rule 34 (b)(1)(C) and (b)(2)(D); Committee Notes on 2006 Rule 34(b) 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

²⁹ *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, PRINCIPLE 6, 118 (2018)

³⁰ *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, Principle 3; comment 3e, 37 (2018)

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

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.” *See* Committee Notes on 2006 Rule 34(b) Amendment (stating, also, “A party that responds to a discovery request by simply producing electronically stored information in a form of its choice, without identifying that form in advance of the production in the response required by Rule 34(b), runs a risk that the requesting party can show that the produced form is not reasonably usable and that it is entitled to production of some or all of the information in an additional form.”).

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 and that data can be stored in several locations including the device itself, in cloud storage, and back-up systems, and the source of the data might impact the appropriate or available form of production. For example, in some cases, mobile device data may need to be processed to a unique format to enable review.
- 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 screen shots, 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 is forensically collected, the data can be produced in either an excel or in short message format, depending on the collection tools utilized, and formats agreed, along with appropriate metadata. Because mobile device data collection is often accomplished using specialized collection software there is a real value to all parties in getting the collection process right from the outset.

These practical considerations along with the requirements established the Rules provide ample justification for an early an on-going 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, end-user data retention, deletion, back-up 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 for mobile device data:

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to

comments@sedonaconference.org

- Short message format: communications or conversation blocks (e.g., RSMF) with files/emojis/attachments divided into fixed blocks of time).
- Individual messages: individual text messages, mobile messaging app messages, or other messages collected from the device and a logical produced individually rather than grouped as conversation threads.
- Mobile device screenshots: suitable for mobile applications (e.g., Signal, Telegram) that are not captured through traditional mobile device collection methods.³¹
- Excel spreadsheet: Text messages and other messaging data may be produced in spreadsheet format. Additionally, this format may be suitable for contact lists and call logs.
- Native file production (suitable for audio, video, pdf Word document and other files shared via mobile devices) and parties may need to produce communications using one or a combination of these forms for various reasons to be conferred upon by the parties.

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 almost universally the subject of discovery discussions and productions is text messages. Despite the ubiquity of mobile device message, 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 the production. As a result, litigants currently work through these production format questions on a case-by-case basis with limited guidance from courts.

A common issue that arises with respect to production format for text messages is whether unitization—how to break down conversation threads for purposes of production. Parties should consider whether to produce the entire conversation thread as a complete “document,” or just a single responsive message, without any context. Other options may include production of message threads by conversation day, 24-hour period, a fixed number of messages before and after a responsive message, or some other increment (*i.e.*, a “communication block”).

The limited court opinions that discuss the production format of mobile device data make it clear that context matters. In *Al Thani v. Hanke*, the court noted that “a single text message, standing alone, is oftentimes meaningless without other messages in the text chain to provide context” requiring Defendant to produce unredacted chat logs because they “are relevant to providing context for the

³¹ Any party planning to use mobile device screenshots needs to consider how to properly authenticate sender, recipient, and date later if used as evidence (e.g. stipulation, declaration/affidavit, testimony).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

other messages in the text chain [as well as Defendants'] business dealings, and their pattern of conduct.”³² Also, in *BidPrime, LLC v. SmartProcure, Inc.* the court found that “[r]ather than deeming a portion of the chat log nonresponsive and omitting it, [the defendant] should produce the full chat log.”³³ Similarly, in *Laub v. Horbaczewski*, the court held “text messages should be provided in a manner that provides a complete record as opposed to scattershot texts.”³⁴ Finally, in *Nichols v. Noom Inc.* the court noted 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.³⁵

Thus, parties should consider some form of production that includes appropriate contextual messages.

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 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. It is often necessary for parties to determine the obligation to produce in full families or message threads, and how to define parents and attachments. Additionally, emojis may play a pivotal role in decisions in multiple jurisdictions. For example, in *In re Bed Bath & Beyond Corp. Securities Litigation*, 2023 U.S. Dist. LEXIS 129613 (D.D.C. July 27, 2023), the court denied a motion to dismiss in a securities fraud case where the defendant tweeted a moon face emoji. His followers interpreted this as a message that the stock would go “to the moon,” and either bought or held shares, driving up the stock price. The court stated that “a symbol's meaning may be clarified by ‘the context in which [the] symbol is used.’” (citation omitted).

IX. IMPACT OF PRE-LITIGATION INFORMATION GOVERNANCE CONSIDERATIONS ON MOBILE DEVICE DATA.

From its position on the far left of the EDRM process, Information Governance designs the plots and plants the seeds that grow into the data harvested in litigation. Guidance on appropriate considerations for policy drafters and program designers exists in abundance. This paper does not purport to replace or even update that guidance. However, an understanding of the elements of a mobile device program is essential to an effective approach to discovery, whether that be from the offensive or defensive perspective.

³² *Al Thani v. Hanke*, No. 20 CIV. 4765 (JPC), 2022 WL 1684271, at *2 (S.D.N.Y. May 26, 2022)

³³ *BidPrime, LLC v. SmartProcure, Inc.*, No. 1:18-CV-478-RP, 2018 WL 6588574, at *2 (W.D. Tex. Nov. 13, 2018)

³⁴ *Laub v. Horbaczewski*, 331 F.R.D. 516, 527 (C.D. Cal. 2019) (quoting *Paisley Park Enterprises, Inc. v. Boxill*, 330 F.R.D. 226, 236 (D. Minn. 2019)).

³⁵ *Nichols v. Noom Inc.*, No. 20 CV 3677L GSKHP, 2021 WL 1997542, at *3 (S.D.N.Y. May 18, 2021)

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

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

A mobile device program should be analyzed from both an equipment and a policy perspective. An understanding of what devices and communication practices are part of any party's device ecosystem is a threshold data point for any discovery practitioner. Elements of a comprehensive program are set forth below.

- Organizations should endeavor to apply a consistent mobile device framework (e.g., BYOD, COPE, COBO) to all employees with a business need to access corporate data from a mobile device and strive to minimize departures/exceptions from that framework.
- That framework should be developed with preservation, collection, and discoverability implications in mind and implemented in a mobile device policy accompanied by mandatory employee training to promote compliance and provide education on mobile device communication best practices.³⁶
- Employees should be directed to limit business communications/collaboration to approved mobile device applications/platforms that synchronize data with enterprise-accessible tools.
- Organizations should consider mobile device management (“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.
- Employee onboarding procedures should expressly address the legal and data security implications of business use of mobile devices, including:
 - Potential jurisdictional privacy considerations impacting the use of personal devices for business purposes (*see* BYOD Commentary)
 - Whether to require advance authorization to access corporate information on personal devices.
- Departing employee procedures should account for the potential need to collect and/or retain access to mobile device content that is relevant to an ongoing or reasonably foreseeable legal proceeding.
 - Evaluate mobile data security vs. preservation/collection obligations.

³⁶ The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495 comment. 2.c. (2018).

This working draft document was created for discussion purposes only for the 2024 Midyear Meeting of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). It is not intended for distribution beyond members of the Sedona Working Group Series. Comments are welcome and may be sent by email to comments@sedonaconference.org

Whether they are responding to or seeking discovery, attorneys should invest the time sufficient to have a well-developed understanding of how each party communicates and if that party is a corporation, how it approaches each of the elements above.

Failure to implement a combination of those elements is likely to bring spoliation claims into play. Civil Courts have readily sanctioned parties for spoliation of evidence of communications.³⁷ Likewise, the DOJ, in March 2023, issued a revised Evaluation of Corporate Compliance Programs policy with a clear focus on communications data. As part of the revised ECCP, the DOJ has provided 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 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 in order to preserve and retain them. Similarly, prosecutors will be tasked with evaluating whether there are consequences for employees who refuse to provide access to business data on personal devices and whether any employees have been disciplined for not providing such access. They are to closely scrutinize the company's "policies and procedures governing the use of personal devices, communication platforms, and messaging applications." 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."

Judges in civil matters may have historically been more protective of the privacy interests of individuals in possession of mobile device data but the preservation obligations are similarly expanding as use of mobile devices becomes the most common form of communication.

³⁷ See, e.g., *Miramontes v. Peraton, Inc.*, 2023 WL 3855603 (N.D. Tex. 2023); *Hunters Capital, LLC v. City of Seattle*, 2023 WL 184208 (W.D. Wash. 2023).