

The Sedona Conference WG1 Discovery of Mobile Device Data Brainstorming Group Outline

Brainstorming Group Members

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

Team Leaders

Dennis Kiker	Michelle Newcomer
--------------	-------------------

Steering Committee Liaisons

Robert Keeling	Kelly McNabb
Maria Salacuse	

Copyright 2023, The Sedona Conference. Reprinted with permission.



This working draft document was created for discussion purposes only for the 2023 Annual 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 dbl@sedonaconference.org

The Sedona Conference Brainstorming Group on Discovery of Mobile Device Data

Discussion Outline

1. Why should there be a paper on this topic?
 - Existing commentary does not provide sufficient guidance for the volumes and types of data increasingly available only on mobile devices.
 - Complex issues regarding possession, custody and control exist in a world where personal and business data are so frequently available on devices often not owned by the litigant.
 - Acquisition of data on mobile devices can be challenging, and guidance is needed regarding what is proportional under the circumstances.
 - Not only are the types of data in mobile devices new and evolving, but the types of mobile devices themselves that Courts are expecting parties to preserve and collect are evolving. Guidance around how individuals and companies should approach the evolution of data and devices is necessary.
 - Discussion Questions
 - Can this guidance be provided via updates to existing commentary (e.g., BYOD)?
2. What is a mobile device for purposes of this paper?
 - Sedona Glossary does not define mobile device.
 - NIST Definition of Mobile Device
 - Discussion Questions
 - Are there certain characteristics that define mobile devices?
 - Should the focus of this paper be on devices or data?
 - How can we make the definition and paper applicable to future innovation?
 - Is it possible to define mobile device in terms of its identity (or lack of identity) with other data sources (e.g., a portable source of unique, relevant information not more easily accessible from a different source)?
 - What mobile devices does this paper not address?
3. What mobile device data does this paper address?
 - As a general proposition, the scope of mobile device data addressed by this paper is the same for devices in the possession, custody, or control of individuals and for devices in the possession, custody, or control of organizations, but differences may exist as to the reasonable accessibility of the data from other sources (e.g., in the case of mobile device management or archiving tools customarily available only to organizations).
 - This paper addresses data that (i) uniquely resides on or is accessible exclusively from a given mobile device; and (ii) data that may be accessible from multiple sources but is more reasonably accessible from a given mobile device than from any other source, weighing established principles of proportionality as well as expectations of privacy.
 - Examples of mobile device data that would typically be in scope under these criteria include locally stored passwords and SMS/MMS messages. Examples of mobile device data that would typically not be in scope under these criteria include emails, chats, and files stored within Microsoft 365 or Google Workspace.

This working draft document was created for discussion purposes only for the 2023 Annual 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 dbl@sedonaconference.org

- The mere fact that this paper addresses a particular form of mobile device data should not be read to suggest a recommendation or presumption as to the discoverability of that form of mobile device data.
 - Discussion Questions
 - What mobile device data does this paper not address?
4. Guidance for identifying mobile devices and determining discoverability of mobile device data.
- Identifying mobile devices
 - Consideration should be given to all potential custodian devices
 - Consideration should be given to interviewing enterprise IT personnel (or others who have access to mobile device data) and monitoring policies
 - Consideration should be given to interviewing custodian for what applications they use for information related to the matter
 - Identifying and conferring on the relevant mobile data sources and understanding the nature of the information those sources contain (prior to collection)
 - Consideration should be given to what the relevant individual data sources are
 - Consideration should be given to what the relevant enterprise data sources are
 - Consideration should be given to as to what appropriate disclosures may be necessary or helpful as to possession, custody or control of the mobile device(s)
 - Impact on PCC of individual v. enterprise devices
 - Impact of a BYOD policy
 - Considerations as to what a reasonable search of mobile devices may include:
 - Cooperation/Transparency Related to Custodial Interviews/Attestations
 - Regarding potentially relevant usage
 - Scope
 - Frequency of communications/usage
 - With who/what
 - Regarding auto-delete settings; deletion practices
 - Regarding back-up data
 - Burden
 - Cooperation/Transparency Related to Searching Methodology
 - Cooperation/transparency regarding Sampling (reasonable verification)
 - Impact of proportionality
 - Discussion Questions
 - Does having this as a separate topic make sense, or should these points be incorporated in the sections below?
5. Guidance for determining preservation obligations for mobile devices.
- What preservations steps are appropriate and adequate for mobile devices?
 - Hold letters (depending on policies below)? Inquiring into retention settings? Mobile device management software installed and used remotely? Transparency into those steps.
 - Impact of company policies on the use/preservation of mobile device data – and timing of disclosure obligations related to same (transparency).

This working draft document was created for discussion purposes only for the 2023 Annual 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 dbl@sedonaconference.org

- How do “possession, custody or control” or “practical ability” affect preservation obligations for personally owned devices?
 - Considerations regarding intersection of data privacy regulations and “processing” information on mobile devices for preservation purposes.
 - What information governance policies/procedures must be implemented to accommodate mobile data preservation?
 - How to handle prospective preservation of data on mobile device.
 - Conducting initial investigation or custodial interview to assess the likely scope of relevant data and ensure that preservation efforts are reasonable and proportional.
 - Is collection necessary to preserve?
 - Cost/burden of collecting to preserve
 - Discussion Question
 - Should preservation of hyperlinked documents including underlying metadata and version history be addressed in this paper or incorporated by reference to another?
6. Guidance for determining appropriate collection methods for mobile device data.
- Collection from a mobile device is recommended when unique data is only available on the device and cannot be collected from a more accessible source.
 - Email and messaging applications like Slack or Teams are typically stored on an external server and may be collected using other means. However, it may be necessary to collect these messages from a mobile device if the server is not accessible or certain messages are cached on the device and only available there.
 - For example, WhatsApp typically only stores 12 months of data in the cloud, but additional messages may be stored on a mobile device.
 - Custodial and IT interviews will provide information on how the device is being used to send and receive information, and what applications are being used. The method of collection depends on the type of applications used and the entity performing the collection.
 - For example, messages sent through an application like Signal may require a manual collection because the data is not otherwise accessible.
 - In a criminal investigation, law enforcement may physically acquire and jailbreak or root the mobile device, whereas, in a civil proceeding, collections are generally logical collections and do not typically require physical possession of the device.
 - Android and IOS mobile devices require different collection methods
 - Forensic collection methods include: (1) a physical collection of the entire device, (2) a logical collection, (3) a file system collection, or (4) a targeted collection of specific folders.
 - The collection methods vary in terms of the type of data they can extract
 - A physical collection will extract: SMS, contacts, call logs, media, app data, files, hidden files, deleted data
 - A logical collection will extract: SMS, contacts, call logs, media, app data
 - A file system collection will extract: SMS, contacts, call logs, media, app data, files, hidden files
 - The method of collection should be determined based on an assessment of the needs of the case, issues of proportionality, and the capabilities of the device. With mobile

This working draft document was created for discussion purposes only for the 2023 Annual 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 dbl@sedonaconference.org

devices, technical limitations may impact the scope of initial collection and cause them to be broader than with other data sources.

- However, more targeted collections can address a custodian's privacy concerns, or may be more appropriate for very small collections of a few screenshots.
- 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.

7. Guidance for determining appropriate search methods for mobile device data.

- **Consider the collection method:** Options depend on how the data was collected, which can range from manual collection of screenshots and individual data files, through forensic extraction of all accessible device data to collection of cloud backups. In some cases, the data can be imported into a forensic tool for parsing of the databases containing common data sources such as call logs, contacts, notes, and text messages.
- **Understanding tool limitations:** Many industry-standard mobile forensic tools do not support search operators such as wildcards or proximity. Moreover, as user-generated text on a mobile device is likely to contain unique abbreviations, emojis as well as typos and erroneously auto-corrected text, relying on strict keyword searches may be ineffective. Where communication data is not threaded, exporting only records with keyword hits may also make it difficult for a reviewer to understand the context. Transcription of media files such as voicemails, audio and video recordings may not be possible in the forensic tool, either.
- **Scoping the search:** Information obtained during custodial interviews may be used to guide the scope of the search, but verification measures may be warranted. For instance, a date range and participants for potentially responsive communications (e.g., SMS/MMS and chats) may be identified. If permitted under the search protocol, a targeted export can then be performed from the forensic tool into an attorney review tool, where more complex searches and additional processing such as near duplicate analysis can be achieved.
- Discussion Question
 - Should paper address why alternative analytical tools such as AI not work well with mobile data?

8. Guidance for production of mobile device data.

- The production format of mobile device data should be discussed at the same time as the parties are conferring about the collection of mobile device data and prior to the collection of such data. The following recommendation assumes the parties agreed on collection of mobile device data.
- There are multiple formats for production of mobile data: chat summaries (conversation blocks such as rsmf or other formats), individual messages, mobile device screenshots and excel files, and parties may need to produce communications using these formats for various reasons.

This working draft document was created for discussion purposes only for the 2023 Annual 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 dbl@sedonaconference.org

- The format that is often easiest to view and produce messaging data is a “chat summary” with files/emojis/attachments divided into blocks of time.
 - Discussion Questions:
 - How do we define “document” in the context of mobile device data?
 - Is this issue being addressed by another paper?
9. Possession, custody, and control issues.
- Defining PCC in the context of mobile devices and mobile device data
 - Jurisdiction and venue may affect decisions and consideration on PCC.
 - Possession v. custody
 - What does control mean?
 - Legal right v. practical ability test
 - Impact of a corporate BYOD policy in determining control—does the policy language matter?
 - Guidance for determining how PCC may impact a party’s obligations with respect to preserving and producing mobile device data
 - Differences between an individual’s obligations v. an enterprise’s obligations
 - Impact of control on a party’s preservation/production obligation
 - Impact of PCC on determining appropriate preservation methods.
 - Discussion Question
 - Is this being covered by another paper?
 - What level of analysis on possession, custody and control is appropriate for this paper?
10. Impact of pre-litigation information governance considerations on mobile device data.
- 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 (see The Sedona Conference, Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations, 19 Sedona Conf. J. 495 (2018), cmt. 2.c. for key provisions) accompanied by mandatory employee training to promote compliance and provide education on mobile device communication best practices.
 - Employees should be directed to limit business communications/collaboration to approved mobile device applications/platforms that synchronize data with enterprise-accessible tools.
 - Mobile device management (“MDM”) and mobile device data archiving tools should be employed by medium-to-large organizations 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, and separating 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.

This working draft document was created for discussion purposes only for the 2023 Annual 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 dbl@sedonaconference.org

- Discussion Questions
 - What is the impact of updated DOJ guidance on company obligations with regard to use of personal devices, and how would that affect corporate policies?

DRAFT