Preserving and collecting mobile device data

By Gareth Evans, Esq., and Nick Snavely, Esq., Redgrave LLP and Tom Seymour, Redgrave Data

JUNE 30, 2022

Mobile devices are ubiquitous, and so is their use to transmit and store information that could relate to litigation or investigations. Yet mobile device data is frequently overlooked by litigants, in part because many attorneys have a limited understanding of how to treat it in discovery.

This article provides a short overview of mobile device data — what it is, why attorneys should care about it, and what they can do to develop a defensible discovery plan for mobile device data.

What is mobile device data?

"Mobile device data" describes electronically stored information (ESI) on mobile devices (smartphones, tablets, drones, etc.). Mobile device data can be stored in device memory (i.e., memory chip(s) soldered to the device motherboard), a SIM card connected to a device, and digital memory card(s) used to store ESI.

Common types of mobile device data include Short Message Service (SMS) and Multimedia Messaging Service (MMS) messages, contacts, call logs, media files, local application data, files, hidden files, deleted files, and raw data stored in device memory.

Mobile Device Data	Description
SMS Messages	A text message of up to 160 characters without an attached file
MMS Messages	A text that includes a file (e.g., picture, video, emoji, link)
Contacts	Contact records stored on the device (e.g., fielded information for different contact records)
Call Logs	Record of incoming and outgoing calls, participants, duration, etc.
Media Files	Photo files, video files, screen captures, etc.
Local Application Data	Applications installed on the device may store unique information (e.g., email messaging, productivity tools, social media)
Files	Files stored in the Files directory of the device memory (PDFs, etc.)
Hidden Files	Files that exist on a system but are "hidden" in the user interface to prevent accidental deletion (e.g., logs, settings files, operating system files)
Deleted Files	Files that have been deleted and may only be available in memory that is unavailable through the API
Raw Data	Byte for byte memory dump of hexadecimal numbers as they existed in device memory (and often unintelligible to the human eye)

Table provided by the authors.

Mobile device data is a significant source of ESI

The explosion of mobile device use is one of the most significant areas of technological expansion over the last decade. Researchers forecast the number of global mobile users to reach 7.49 billion by 2025. (See Statista, "Forecast number of mobile users worldwide from 2020 to 2025," available at: https://bit.ly/3I4GTzG.)

The number of mobile devices and users continue to increase, and evidence suggests mobile devices are supplanting computers as primary devices, with the World Advertising Research Center estimating that 72% of all internet users will solely use smartphones to access the web by 2025. (See World Advertising Research Center (WARC), "Mobile advertising has reached a tipping point," Jan. 28, 2019, available at: https://bit.ly/3AedtgC.)

While the mobile data technology and use landscape is constantly changing, the impact on eDiscovery is not.

New innovations continue to evolve the way mobile devices use and store data, and this presents substantial challenges for discovery given that the ability to access and extract mobile device data varies greatly depending on device hardware, software, operating system, encryption, and chipset.

Mobile device data is a significant discovery issue

While the mobile data technology and use landscape is constantly changing, the impact on eDiscovery is not. As the Sedona Conference observed in its 2018 "Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations," parties "cannot ignore their discovery obligations merely because the ESI is on a device that is mobile[.]"

The legal industry has been slow to recognize the importance of mobile device data, and some attorneys still treat mobile data as presumptively "off the table" in discovery without having thoroughly considered the role of such data in a specific case. Where parties and their counsel do take some steps to preserve or collect mobile device data, those steps can be incomplete, and relevant data may be lost. The result has been a stream of cases in which litigants and their lawyers have been sanctioned for failing to reasonably preserve mobile device data.

A few examples from the first half of 2022 alone:

- In *ORP Surgical, LLP v. Howmedica Osteonics Corp.*, a federal court in Colorado admonished and sanctioned both a party and its lawyers for (among other things) failing to take adequate steps to preserve text messages from two witnesses — even though most (but not all) of the text messages were ultimately recovered.
- In *Schnatter v. 247 Grp., LLC*, a magistrate judge in Kentucky recommended that the founder of the Papa John's pizza chain be sanctioned for failing to preserve mobile device data because, although he had provided two personal phones to counsel for imaging on separate occasions, he had used other phones during the relevant period that were not preserved, and he had deleted text messages.
- In *NuVasive, Inc. v. Day*, a federal court in Massachusetts awarded judgment and damages to a plaintiff based, in part, on an adverse inference that the court applied because the defendant obtained a new phone shortly after receiving a litigation hold notice but set the phone to automatically delete text messages.

The lesson from these cases and others like them is not that a litigant must capture and produce every bit of data from every custodian's mobile phone in every matter. Rather, attorneys should carefully evaluate what reasonable steps their clients should take to preserve mobile device data in light of the unique circumstances of their case — and should familiarize themselves with the available options for preservation and collection so they can select the ones that are right for their matter.

As mobile device usage continues to expand and the tools and options for the preservation and collection of mobile data become more sophisticated, attorneys should not treat mobile data as an afterthought.

Options for preserving mobile device data include:

- **Notifying custodians** about their obligations to preserve (and instructing them to preserve) information relevant to litigation or investigations stored on their mobile device. This action is a baseline preservation effort, but it may still be (and often is) reasonable. Depending on the circumstances, it may be appropriate to take other steps to preserve information rather than relying on each custodian to preserve their own information in place.
- **Proactively capturing** and preserving copies of certain mobile device data with a purpose-built application (e.g., journaling all SMS or WhatsApp messages sent and received to/from mobile devices and storing those messages in an archive). This action is a robust option that may help avoid the need to preserve and collect information stored on individual mobile devices, but it likely requires substantial capital and investigation to implement and maintain — and it will likely preserve far more information than is necessary.
- **Collecting** mobile device data is also a preservation option. Depending on the matter, the extraction methods described below could be used to preserve information.

There are multiple methods for extracting ESI from mobile devices. The feasibility of each method depends upon the make, model, and operating system of the mobile device. No one technology can access and extract all data from all mobile devices, and no one type of extraction has guaranteed success.

Methods to extract ESI from mobile devices include:

- **Manual extraction** methods access data through the device interface and manually capture copies of the ESI (e.g., create screen captures or recordings, filming the device screen during the investigation). While this may be the easiest approach and might be appropriate in some matters involving a small volume of ESI where metadata and searchable text are not needed, it may become impractical as the number of devices and the volume of ESI increase. Because this method does not yield searchable text, does not preserve or extract metadata, and may present admissibility challenges, it will not be a viable option in most circumstances.
- **Logical extraction** methods utilize forensic software that interacts with the mobile device operating system through an application programming interface (API) and extracts only active data that is accessible through the API. This method extracts most live data (e.g., SMS/MMS messages, contacts call logs, media files, and local application data) and it is the fastest and most widely supported "forensic" collection method.
- **File system extraction** methods utilize forensic software to access data on the device without an API, and they extract all files present in the internal memory, including those inaccessible through the API. This method extracts all files from device storage, including logs and system files, that may not normally be visible to a user. This method requires gaining access to the root storage and takes longer compared to a logical extraction.
- **Physical extraction** methods utilize forensic software and full access to the internal memory of the mobile device. A physical extraction performs a bit-by-bit copy of the device's memory. This option is the most comprehensive extraction method and will include deleted files and fragments that would not be included in a logical or file system extraction.
- **Hardware forensics** methods like chip-off extraction and microscope reading utilize specialized software and hardware to inspect the physical components of a mobile device to identify and extract data. These extraordinarily complex, time-consuming, and expensive methods would only be utilized in the most extreme and narrow circumstances.

Conclusion

As mobile device usage continues to expand and the tools and options for the preservation and collection of mobile data become more sophisticated, attorneys should not treat mobile data as an afterthought. While the preservation and collection approach selected can and should vary in different cases, counsel should be prepared to:

- Familiarize themselves with available preservation and collection methods, tools, and technologies, including what categories of data are preserved or collected by each option.
- Conduct a reasonable inquiry as early as possible in the litigation to determine:
  - What, if any, mobile data is within a client's possession, custody, or control — taking into account both the legal standard in the relevant jurisdiction and the client's device usage policies;
  - The likelihood that mobile device data is both relevant and unique (does not exist from other sources);
  - The importance to the issues in the case of any relevant, unique mobile data; and
  - The burden or difficulty of collecting mobile data — including complications such as privacy restrictions on accessing personal devices.
- Choose what methods of preservation and/or collection are appropriate and defensible in light of the circumstances of the case (e.g., data on the phone of a central figure may be treated differently than that of ancillary custodians).
- Consider negotiating with the opposing party a reciprocal discovery approach that applies to both parties' mobile data.

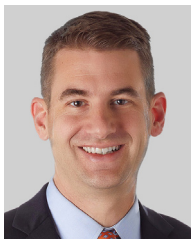
Counsel may also be well served to obtain the assistance of knowledgeable and experienced eDiscovery counsel or consultants to help navigate the complex legal and technical issues that arise in connection with the preservation and collection of mobile device data.

	Screen Capture	SMS/MMS Messages	Contacts	Call Logs	Media Files	Local App Data	Files	Hidden Files	Deleted Files	Raw Data
Manual Extraction	●									
Logical Extraction		●	●	●	●	●				
File System Extraction		●	●	●	●	●	●	●		
Physical Extraction		●	●	●	●	●	●	●	●	
Chip-Off Extraction										●
Microscope Read										●

Table provided by the authors.

About the authors





Gareth Evans (L) and **Nick Snavely** (C) are partners at **Redgrave LLP**, where they counsel clients on complex matters related to information law, which includes eDiscovery, information governance, and data privacy and cybersecurity issues. They are based in Los Angeles and Chicago, respectively, and can be reached at gevans@redgravellp.com and nsnavely@redgravellp.com. **Tom Seymour** (R) is the director of Strategic Consulting at **Redgrave Data** where he designs targeted technology and workflow solutions to address clients' eDiscovery and information governance needs. He is based in Kansas City, Kansas, and can be reached at tom.seymour@redgravedata.com.

This article was first published on Reuters Legal News and Westlaw Today on June 30, 2022.