The Legal Intelligencer

Insights for Attorneys Handling Mobile Devices During Discovery

By Tess Blair, Tara Lawler, William Childress and Leonard Impagliazzo

L-R: Leonard Impagliazzo, Tess Blair, Tara Lawler and William Childress of Morgan Lewis & Bockius. Courtesy photos

December 2, 2022

Discovery involves the preservation, identification, collection, and production of potentially relevant, nonprivileged information. The discovery process is not complex, but it does require strategy as each organization has its own unique data landscape and each case requires careful and thorough analysis and control of the scope of a party's discovery obligations.

A decade ago, email systems were the primary source of discoverable electronically stored information (ESI). EData attorneys, in conjunction with technologists and IT professionals, have developed streamlined and repeatable processes for preserving, identifying and collecting potentially relevant emails. Because of this progress, email collections are now ubiquitous and usually straightforward, at least for larger organizations with internal discovery capabilities.

Growing pains persist, however, in preserving, collecting and producing information from other sources. Mobile devices are undoubtedly a current pain point in the discovery process. In this article, we address some practical considerations that every eData attorney should consider when handling mobile devices during discovery.

Today's mobile devices are handheld computers that connect us to co-workers, friends, family members and the world. The devices are a repository for our videos, photos, notes, and conversations that include both mundane and sensitive information. We use our devices to search the web, interact on social

media, shop, consume news and navigate our travel. The average person is rarely separated from his or her mobile device—if not in our hand, then in our pocket, and nearly always within arm's reach, even when we're asleep.

In the hands of a capable eData attorney, a mobile device can reveal a nearly complete chronology of the owner's personal and professional life, complete with people, places, pictures, and commentary. Thus, mobile device discovery must be approached cautiously, with a device's content carefully considered for uniqueness and relevance before any agreement is made to discover its content. Indeed, because of the ubiquity of mobile devices in our lives, privacy must be a paramount concern. Therefore, the first question to ask is whether the device contains unique and relevant data that cannot be obtained from other sources. If there is no unique, potentially responsive data on the device, then it is best to move on to other data sources, especially when so much private information can be swept up during a mobile device collection. For example, if an individual's work email resides on her mobile device but is also synched to her company's email server, then any potentially responsive emails should be collected from the company email server, not the mobile device.

Early in a case, litigants will likely be uncertain about whether mobile devices are implicated. Nevertheless, caution requires providing potential custodians clear and practical legal hold instructions on preserving mobile device data. Mobile devices can be preserved with instructions to refrain from resetting the device or purging data and clear instructions on how to back up all potentially relevant data on the device. Text messages are an area that can be particularly problematic. Some custodians may use the auto-delete function intentionally or inadvertently because they are unaware that in order to back up text messages a manual adjustment in the custodian's settings might be required. If mobile device data is a potential source of discoverable data in a case, the legal hold notice should address preservation and instruct custodians on how to utilize cloud-based technology, override any auto-delete functions, and manually turn on automatic backup features. Providing practical instructions will facilitate the backup of mobile devices to cloud-based storage applications such as Google Cloud, iCloud, Dropbox and OneDrive.

As part of issuing a legal hold, eData attorneys should also use well-crafted mobile data surveys or conduct custodial interviews. Understanding whether the custodian has used the mobile device to communicate about issues potentially relevant to the case can help determine whether preservation and collection are necessary. Surveys and interviews also provide another touchpoint for instructing custodians on how to disable auto-delete settings and enable automatic backups.

Unless the eData attorney has determined that there is a clear risk that potentially relevant and unique data residing on a mobile device will be lost or destroyed, preservation in place can be a defensible and reasonable substitute for collecting the data until a determination is made on whether a collection is needed.

When collecting mobile device data, consider whether the device is a company-owned device, a personal device operated through a company's bring your own device (BYOD) program, or a purely personal device—the answer will determine how to approach the collection. If the device operates under a BYOD program, the eData attorney should review the client's BYOD policy to ensure compliance with the policy when seeking access to the device. BYOD programs typically provide notice to employees on the type of applications and data that the company is monitoring and may access for its business and legal purposes.

When a collection is necessary, the average custodian may be hesitant to give unfettered access to his device, unless the device has been used solely for work purposes. Unlike other types of ESI collections such as hard drive imaging or collection of email data, mobile device collections require the cooperation of the custodian since the device is typically in the sole possession of the custodian and access is controlled by a passcode, which typically only the custodian knows.

In this situation, the eData attorney should be sensitive to the custodian's concerns. Indeed, be prepared for foot dragging and occasionally a refusal to provide access to a device. In many instances, thoughtful collection interviews can help to alleviate resistance. For example, working with a custodian on identifying and collecting specific text threads that are relevant or particular contacts with whom the custodian had relevant conversations can drive home the point that no one is interested in reading irrelevant personal text messages exchanged with social contacts. A clear explanation of what is needed for the matter and why it is needed will be better received than a cryptic command to hand the phone over for collection.

Obtaining access to the phone is only the first hurdle. The mechanics of identifying and collecting data sources residing on a device can be complicated. Mobile device data includes not only text messages, call logs, contacts, and notes, but also third-party messaging platforms such as Telegram and Signal. These third-party messaging platforms and the ephemeral nature of some of these platforms can create preservation challenges. The eData attorney should understand the hurdles that these third-party messaging platforms create and how to collect data from each, if necessary.

In some litigations, if a mobile device contains a small set of unique, potentially relevant information, obtaining screenshots of the potentially relevant information, such as text messages, could be an acceptable alternative to a forensic collection. The screenshot capturing process needs to be managed carefully since screenshots can be altered or fabricated. Manipulation of messages prior to taking a screenshot is possible because some messaging platforms allow for deletion after the message is received and read. In addition, screenshots can be altered by general photo-altering software and, in some instances, can be fabricated using applications designed to replicate messaging applications. Therefore, as part of the collection, some verification should be done by the eData attorney to confirm that the screenshots are accurate representations of the original messages on the device. The eData attorney should also understand that screenshots will not capture metadata, which can indicate if a message has been altered. Even if screenshots are determined to be acceptable for a particular case, the eData attorney should also ensure that the custodian knows that he or she must take reasonable steps to ensure the original information continues to be preserved. If later compelled to conduct a forensic collection of the device, preserving the original data in place is necessary.

The eData attorney's awareness of common messaging applications is crucial to creating a defensible collection plan for mobile device data. The eData attorney must be able to distinguish between applications that are designed to store data locally versus those that are designed to store data elsewhere and merely be viewable on the application. The ability to access raw mobile device data is a key factor in the decision-making process on whether to conduct a full forensic collection or balance the risks of collecting through screenshots.

After mobile device data is collected, several considerations inform the processing, review, and production of this content. Traditional discovery processing engines utilize algorithms and specialized workflows to retrieve metadata and allow for ingestion of data, such as email, images, documents, and unstructured data. Processing mobile device data may be complex given the two competing operating

systems: Android and iOS. Current discovery processing engines may have differing capabilities and limitations on handling the operating systems. If the processing engine can handle the mobile device data collected for the matter, consider the format in which the data will be viewable. Will each message present itself as an individual document? How will items such as photos, GIFs, and emojis appear? Will chat threads be discernable or will each individual custodian's text messages appear to be one long unending thread?

Depending on the processing engine and review platform, specialized technology may be needed to deal with certain messaging applications. In addition to understanding the technical specifications of each application on the mobile device, the eData attorney should consider the need to utilize additional software and applications to enrich the review and production capabilities of the mobile device data.

For example, text messages are often converted into relativity short message format (RSMF). RSMF allows for conversion of data from applications such as SMS, Apple iMessage, Skype, and Bloomberg, which provides for messages to be viewable similar to a conventional document. RSMF allows for utilization of a viewer and may offer support for grouping text message threads together, identifying read receipts, chat history, and icons or emojis.

Next, the eData attorney should consider how text message threads should be grouped together. The grouping of text message threads together allows for the creation of messaging transcripts. With RSMF there is the ability to customize the intervals in which a transcript may start and end. Some of the more widely used intervals are eight-hour and 24-hour transcript threads. To date, no uniform standard for time intervals has developed in practice.

The eData attorney must consider the specific needs of the litigation, as well as certain logistics such as production deadlines, protective orders, privilege logs, budgeting, and cooperation with opposing counsel. Protective orders and ESI protocols may limit or expand the ability to redact nonresponsive and/or personal information in addition to addressing the scope of a privilege log. The eData attorney should be strategic in leveraging protective orders and ESI protocols in determining intervals for messaging transcripts. If redactions for nonresponsive and personal information is permitted, a longer transcript for a longer period might be preferred. The longer transcripts will lead to "less documents" but may also require more redactions to be made, whereas shorter transcripts are likely to lead to "more documents," but potentially be less redaction-intensive. A shorter transcript document with no responsive information can be treated as not responsive and discarded from any future production. Even after the eData attorney has considered the particulars of the applicable protective order and ESI protocol, he or she should think strategically to determine messaging transcript length to ensure utilization of the most efficient and economical review-to-production workstream.

The eData attorney should also consider the potential for privileged conversations to be present throughout messaging platforms. Not only could messages implicate the need for redactions, but they also may call into question the validity of the privilege if conversations extend beyond the attorney-client relationship. For example, custodians who maintain a personal relationship with their attorney and often exchange personal conversations with legal advice scattered throughout may lead to challenges from opposing counsel as to whether the messages were obtained for the purposes of seeking or providing legal advice. This type of sporadic request or provision of legal advice may make crafting a privilege basis that does not reveal the nature of the legal advice sought or received particularly challenging, given the short length of text messages. The eData attorney will also need to

consider the logistical question of whether each message needs to be logged individually with a supporting privilege basis or if an uninterrupted chat thread should be treated as one entry.

The collection, review, and production of mobile device data can present practical and technical challenges for even the most experienced eData attorney. Each mobile device collection should be approached carefully and tailored to the specific needs of the litigation. Precise strategy and advanced planning, as with most discovery tasks, will allow for the efficient, consistent and defensible production of mobile device data.

Morgan, Lewis & Bockius partner **Tess Blair** *is the founder and leader of the firm's eData practice. Partner* **Tara Lawler***'s practice focuses on e-discovery, information management and data privacy. Associate* **William Childress** *counsels clients on electronic discovery and associate* **Leonard Impagliazzo***'s practice also focuses on e-discovery, information management and data privacy.*