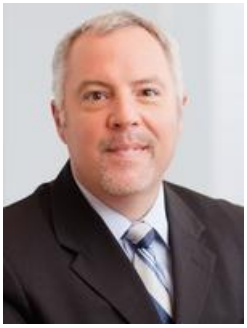
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

How Mobile Devices Are Changing E-Discovery

Law360, New York (March 17, 2016, 10:52 AM ET) --
Legal practitioners can no longer afford to ignore the importance of mobile device data in discovery, investigations and other proceedings. Mobile devices such as cellphones, smartphones, e-readers and tablets pose a significant and unique challenge to the legal industry when it comes to the collection, searching, processing and production of electronically stored information for discovery.


Jon Kessler


David Rohde

In the U.S., for instance, 90 percent of employees utilize their personal smartphone for work purposes[1]. There is growing acceptance among the industry that this is posing a unique challenge. However, practitioners need to respond quickly, placing these developments in the context of the amended Federal Rules of Civil Procedure to address proportionality issues under Rule 26[2] and to seek the benefits potentially conferred by Rule 37(e)[3].

Unlike computers and servers, mobile devices can't simply be "cracked open" and copied or forensically imaged bit-by-bit. Every model is somewhat unique. Numerous issues must be addressed, including the type of dispute or investigation, commingling of personal and business data, mobile data storage in the cloud, the manufacturer of the device and its operating system, mobile device management (MDM) software, data protection and encryption, and the type of data being sought. Further, investigative matters may also require specialized radio frequency (RF) isolation containers when collecting a device. Failure to properly shield it from RF signals such as Wi-Fi, Bluetooth and cellular service could result in a user executing a remote "wipe" or the operation of predefined retention policies.

Given this backdrop, here are four key areas for consideration when approaching mobile data collection.

BYOD and COPE Devices

"Bring Your Own Device" (BYOD) is an established and growing trend in the business world due to its potential for cost savings as well as its popularity among end users seeking to carry a single device of their choosing for business and personal connectivity. This usage creates complex e-discovery and security issues due to personal data being commingled with confidential, proprietary and/or sensitive business data. When e-discovery obligations require collection from BYODs, sensitive issues often

surface regarding custody, control, ownership and safeguards to preclude review or disclosure of personal information[4]. A broad collection is often necessary because of the insufficiency of technical or logical boundaries between personal and business data on the device.

As a result of these issues, businesses have recently turned to "Company Owned but Personally Enabled" (COPE) devices. COPEs are corporate/carrier-owned mobile devices used in the workplace, whereby both workplace and personal data are permitted, but both types of data are regulated by corporate policy. While COPE devices provide more control over employee devices, privacy concerns still remain.

Identifying devices that require collection may be accomplished through either a custodian interview process or by more automated approaches. In some cases, attorneys make the decision to collect all content from all mobile devices, regardless of scope. This method is not always the best approach, as the entirety of the mobile device often does not contain even potentially responsive information. Corporate email is a prime example of content on a mobile device that may not need to be collected from the device. Corporate email is almost always synchronized between the device and the corporate server, making that server the best and most complete record.

Text ("SMS") messages are another good example of data that may exist on mobile devices, but may not be relevant to the inquiry at hand, and should not *always* be collected. In most cases, the data required for preservation, review and production is focused on a particular substantive topic, whereas SMS messages could be very general, broad and not relevant.

Careful consideration of the privacy, relevancy, costs and burdens involved in mobile device data collections should be observed in order to limit collections to only responsive mobile data.

New Text Messaging and Chat Applications

Mobile device messaging has evolved significantly since the early days of SMS texts. Many different proprietary and third-party applications can be used to communicate and store messages in text and multimedia formats. An e-discovery collection request simply targeting "text messages" doesn't cut it anymore. Different collection methods and tools will vary with regard to the amount and type(s) of data they are able to collect on different devices and from third-party applications — the wrong tool or collection method can result in incomplete, missing or incorrect data — even when there is data in those applications. It is

Potentially Responsive Data Found On Mobile Devices

- Text Messages
- Chats
- Call logs
- Contacts/address books
- Emails
- Photos
- Videos
- Notes
- Recorder memos
- Saved documents
- Voicemails
- GPS Locations
- Calendars
- Internet history
- Search engine history
- Social media artifacts
- System logs
- User activity metadata
- Third-party applications which can also contain all of the items mentioned here within them

Whether or not they are important to your case, or to the negotiation of a discovery protocol are decisions best made from an informed perspective, and on a case-by-case basis. What is not in doubt is that mobile device data can be, and often is discoverable. City of Ontario v. Quon, 130 S. Ct. 2619 (2010); EEOC v. Original Honeybaked Ham Co. of Georgia Inc., No. 11-cv-02560-MSK-MEH (D. Colo. Nov. 7, 2012).

almost a full-time job to keep up with messaging platforms and services available to mobile device users today. Popular platforms such as WhatsApp, Facebook Messenger and Snapchat, to name but a few, have changed the messaging landscape with significant implications for the e-discovery process. Geography, type of device, state of connectivity (i.e., Wi-Fi or cellular), age and demographic of user, and many more factors combine to make "messaging" an even more complex and fast-changing environment.
In addition, many of these apps are cross-platform, and can be used on Apple iOS, Android, Windows Phone and Blackberry devices.

Knowing what you are looking for and what messaging platforms are in place can help make the mobile device collection and the subsequent representations made by counsel about the completeness and correctness of the eventual production more defensible. Failure to preserve or produce responsive content can have serious consequences.[5]

Focus on Social Media and Cloud Storage

Social media and data stored in the cloud are typically collected using defined protocols. It is important to understand, however, that mobile devices are key access points to these services by users away from the web-based portal or installed application on a desktop or laptop computer. Social media artifacts and cloud storage evidence are resident on mobile devices and could yield important information for your case. This could include information ranging from additional user communications to evidence of cloud-based storage repositories potentially used to upload information responsive in your matter — for example, proprietary company documents and intellectual property. Important discovery considerations include the retention period in effect for subject content at various cloud providers, determinations of custody and control, and deploying the right tools at the right time to accomplish preservation and collection.

Fast-Changing Mobile Device Technology

Mobile devices are typically heavily subsidized by either the device manufacturer or the cellular carrier tying them to contract-based service agreements. This arrangement allows users to replace their devices on a regular cycle of one to two years — ensuring that the user always has the "latest and greatest" device. Software updates to those devices (both the operating system and the application resident thereon) happen much more frequently. Some are even pushed out in an automated fashion, prompting the user to update his or her device with the simple touch of a screen. There are thousands of mobile devices in circulation with software updates released on a daily basis. Forensic software is always playing catch-up to reverse-engineer data storage methods to allow collection and presentation of mobile device data.

Due to this highly dynamic technology truism, no single piece of forensic software is the answer to all mobile device collection and data extraction needs. Forensic software packages are updated as new issues are found to allow for up-to-date parsing of the content they have currently reverse-engineered. On a particular device, the forensic software update may allow SMS messages to be parsed, but require a different forensic software product for a third-party message store, therefore defining the potentially responsive information prior to the collection process is paramount and ensures preservation is complete and appropriate.

Mobile devices play an increasingly important part in both home and work life. As connected devices that capture data continue to proliferate (with forensic toolkits now supporting more than 10,000

different devices), legal practitioners will face challenges as they try to stay abreast of both the technology and the law. It is important that attorneys understand the rapidly changing landscape of mobile devices, their relative import to a matter, and the obligations, costs, burdens and benefits associated with accessing those devices in the context of litigation.

—By Jon Kessler and David Rohde, Epiq Systems Inc.

Jon Kessler is senior director of forensics and collections and David Rohde is senior director of consulting services at Epiq Systems.

---

[1]https://iapp.org/media/pdf/knowledge_center/Cisco_BYOD_Insights_2013.pdf

[2] Whereby proportionally requirements are now "baked in" to the scope of permissible discovery and limit "fishing expeditions." See generally, Federal Rules of Civil Procedure (FRCP) Rule 26 and related Committee Notes.

[3] Whereby a "safe harbor" is provided for producing parties taking reasonable steps to preserve ESI. See generally, Federal Rules of Civil Procedure (FRCP) Rule 37(e) and related Committee Notes.

[4] These considerations are heightened for collection and other processing of certain personal information in jurisdictions outside the U.S.

[5] *United States v. Vaughn*, No. 14-23 (JLL), 2015 WL 6948577 (D.N.J. Nov. 10, 2015); *In re Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig.*, MDL No. 2385, 2013 WL 6486921 (S.D. Ill. Dec. 9, 2013); *Southeastern Mechanical Services, Inc., Plaintiff, vs. Norman Brody, et al., Defendants*, 2009 U.S. Dist. LEXIS 85430.