Be Smart: Mobile Devices and Forensic Imaging

Scott J. Etish

The Legal Intelligencer, March 22, 2016

Even before the adoption of the original e-discovery-related amendments to the Federal Rules of Civil Procedure in December 2006, litigants regularly sought forensic copies—or images—of computer hard drives in the discovery process, particularly when there was a risk of loss of evidence. In the early days of e-discovery, the decisional law on the right to and scope of such (then) extraordinary discovery primarily focused on requests for imaging of computer or portable hard drives.

However, with the explosion in the use of mobile devices, and their extension of the trail of relevant electronically stored information (ESI), there has been an increase in requests for imaging of mobile devices, and legal opinions that address these requests. This trend promises to continue considering the vast array of information available on smartphones, tablets and other portable devices, which now includes email; text and voicemail messages; call history; browser (Internet search) history; photographs; video and voice recording; GPS data; cellular and Wi-Fi location history; and maps and navigation history, according to "The Big Data Collection Problem of Little Mobile Devices," by Michael Arnold & Dennis R. Kiker.

This vast array of available data, combined with the proliferation of corporate "bring your own device" (BYOD) practices and policies, will make device imaging a common practice. This article discusses recent court decisions addressing requests for forensic imaging of an adversary's mobile device.

Federal Rule of Civil Procedure 34 permits a party "to inspect, copy, test, or sample any designated documents or electronically stored information."

The official Comment to Rule 34 and case law since the 2006 Federal Amendments make it clear that forensic imaging, while much more common in recent years, is still typically considered an extraordinary request that will generally be permitted only in exceptional circumstances. The recent amendments to Federal Rule of Civil Procedure 26(b)(1), which became effective Dec. 1, 2015, will likely not make it any easier to secure an order requiring the

imaging of a party's electronic device. Pursuant to the pre-amendment rule, "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense." However, under the new rule:

"Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit."

The "subject matter" and "reasonably calculated" openers—two clauses often misinterpreted or misapplied by practitioners to open the floodgates on discovery—have also been removed. Combined with the central change of explicitly incorporating the concept of proportionality, these revisions to Rule 26 will likely make it even more difficult to secure an order requiring the imaging of an adversary's mobile device.

Cases Involving Requests to Image Adversary's Electronic Devices

Courts will generally not require a party to turn over a mobile device for a forensic inspection or imaging in the absence of exceptional circumstances. As expected, many of the cases addressing requests for forensic imaging of mobile devices draw heavily upon earlier cases involving forensic imaging of a party's hard drive. While the burden is high, parties are more likely to be successful in seeking to image an adversary's electronic device when they are able to demonstrate that they have been unable to obtain the information through traditional discovery methods (i.e., a party has failed to fulfill its discovery obligations by intentionally or negligently deleting relevant ESI), as held in Genworth Financial Wealth Management v. McMullan, 2010 U.S. Dist. LEXIS 53145 (D. Conn. June 1, 2010).

In Genworth, the plaintiff presented evidence that one defendant used his personal computer and personal email address to download, access and transmit the plaintiff's proprietary information. The defendant further admitted that he spoliated evidence when he discarded his computer even after counsel instructed the defendant not to do so. Accordingly, the plaintiff was able to demonstrate that a forensic imaging of the defendant's electronic devices was required because of the defendant's spoliation.

Courts have also not hesitated to sanction parties in situations involving a party's failure to preserve relevant ESI from mobile devices such as text messages, as in Calderon v. Corporacion Puertorriquena De La Salud, 992 F. Supp. 2d 48, 50 (D.P.R. 2014), and inChristou v. Beatport, 2013 U.S. Dist. LEXIS 9034, at *37-39 (D. Colo. Jan. 23, 2013). Recent decisions also demonstrate that courts will be more inclined to order a party to turn over an electronic device for forensic imaging when the operation and/or content of a computer, mobile device and/or computer system is directly related to a cause of action, as in Ameriwood Industries v. Liberman, 2006 U.S. Dist. LEXIS 93380, at *6 (E.D. Mo. Dec. 27, 2006).

There are very few situations in which a litigant should not be specific when seeking relief from the court, and this is certainly true when seeking access to an adversary's mobile device. Litigants should describe in detail the relevance of the electronic evidence being sought, as in Freres v. Xyngular, 2014 U.S. Dist LEXIS 44116 at *14 (D. Utah Mar. 31, 2014), and in Bailey v. Scoutware, 2014 U.S. Dist. LEXIS 37197, at *17-18 (E.D. Mich. Mar. 21, 2014).

For instance, in Bailey, a whistleblower and breach of contract action, the plaintiff alleged that the defendant terminated and breached its contract with him after discovering he had filed a suit against his former employer, Fast Model. In discovery, the parties disputed the discoverability of several text messages between a Fast Model employee and the plaintiff's co-worker/mentor at Scoutware. These text messages allegedly occurred shortly after the plaintiff's deposition in the case against Fast Model after Fast Model first learned that the plaintiff was employed by Scoutware. Scoutware did not produce the text messages and alleged that it could not recover them. However, it later clarified that it had asked an expert to review the plaintiff's co-worker's phone, but the expert could not recover the text messages or any voice messages. The plaintiff applied to the court seeking an order, inter alia, requiring Scoutware to turn over the cellphone at issue for examination by his expert. The plaintiff argued that the five missing and two available voice messages were the only recorded pieces of evidence pertaining to the communications between plaintiff's former employer and current employer.

Acknowledging this specificity and the relevance of the evidence, the court allowed the imaging, explaining that "if defendant had the cellphone in its possession and was able to examine it with an expert, that plaintiff also should have the ability to examine the phone."

In contrast, mobile device imaging and examination requests are likely to be denied where the request is broad in nature, and where the request is based on a "mere suspicion" that the responding party is withholding ESI from production, as in A.M. Castle & Co. v. Byrne, 2015 U.S. Dist. LEXIS 106146 (S.D. Tex. Aug. 12, 2015), and in Babcock Power v. Kapsalis, 2015 U.S. Dist. LEXIS 168709 (W.D. Ky. Dec. 17, 2015).

Practice Tips

These decisions emphasize the general rule that while forensic examination remains an extraordinary discovery device, such requests are more likely to be granted where a party is able to demonstrate that they have been unable to secure the requested information through traditional discovery. Applications for a forensic imaging of a mobile device will often be aided by evidence demonstrating the inability to retrieve the requested evidence from other, more traditional data sources, a party's failure to comply with their discovery obligations, failure to preserve devices (despite explicit requests to opposing counsel requesting the same), or unusual computer use and data management practices. A party must be specific in identifying both the evidence sought, and the rationale for seeking it from these atypical sources.
While a party may be inclined to seek mobile-device discovery based upon the mere suspicion that evidence exists and is being withheld, such suspicions, without more, are very unlikely to carry the day on a motion. As courts become more familiar with mobile devices as legitimate discovery sources, litigants would be well-served to develop a record supporting both the "sole location of discovery" and spoliation/discovery abuse arguments before seeking the court's intervention.