Privacy vs. the Need to Collect Evidence from Smartphones

What does your commercial litigation client have to hide?

Jonathan S. Liss, Frederick W. Alworth and Christine A. Amalfe

New Jersey Law Journal, May 23, 2016

For a litigator, few moments compare to when you find the "smoking gun" that blows a litigation wide open. But now, more often than not, smoking guns are on an individual's smartphone. How is data (such as emails, text messages and instant messages) from smartphones discoverable, and what do you need to show to obtain such access? Also, is a company that is served with a demand for discovery required to produce smartphone data from its employees' personal devices?

Imagine a client's horror when you tell them that they have to turn over their phone to an adversary. Plus, New Jersey courts have not provided clear guidance on how the rules are to be applied when a civil litigant seeks text messages. That said, recovery of data from smartphones is particularly important because, unlike email, which is typically recoverable from other primary locations, generally text messages can be obtained only from the smartphone, as cloud-based service providers (Verizon Wireless, AT&T, etc.) retain the contents of text messages only for a short period of time.

The Lack of Clear Standards: What Do You Need to Show?

In any discussion of the standards, the first place to look is the New Jersey Court Rules (if the matter is in state court) and the Federal Rules of Civil Procedure and our Local Rules (if the matter is in federal court). Both the New Jersey rules and federal rules provide for the discovery of documents relevant to a party's claims, including smartphone data. N.J. Ct. R. 4:10-2(a); Fed. R. Civ. P. 26(b)(1). While electronic data is discoverable, both the New Jersey rules and federal rules provide exceptions for electronically stored information (ESI) that is not reasonably accessible because of undue burden or cost. N.J. Ct. R. 4:10-2(f); Fed. R. Civ. P. 26(b)(2)(B). In addition, both the New Jersey rules and federal rules (following the 2015 amendments) require that the discovery be "proportional" to the needs of the case. N.J. Ct. R. 4:10-2(g)(3); Fed. R. Civ. P. 26(b)(2)(B).

The rules also require the parties to identify issues regarding ESI at the earliest stage of the litigation. See Local Rule 26.1(d); N.J. Ct. R. 4:5B-2. To that end, we recommend that, in the initial litigation hold to one's adversary, you specify the need to retain smartphone data and you likewise advise your client of the need to retain this information.

While the data on smartphones might be technically discoverable, in today's world, where people's "lives" are on their phones—health, family and other ultra-personal information—courts are reluctant to order "turnovers" of phones. The U.S. Supreme Court recognized these privacy concerns in *Riley v. California*, 134 S. Ct. 2473 (2014), where it held that, in the criminal context, the police may not search without a warrant a smartphone that is seized during an arrest, unless exigent circumstances are present.

But, in the civil context, what if the smartphone was used to communicate on issues relevant to the case? Courts around the country are grappling with these issues, and New Jersey judges are dealing with this cutting-edge concern on an ad hoc basis by trying to balance discoverability, costs and litigants' privacy concerns.

Several cases outside New Jersey provide some guidance in the employment context. In *Bakhit v. Safety Marketing*, (D. Conn. June 26, 2014), a court, relying on *Riley*, denied a request to inspect smartphones based on privacy concerns. Similarly, in *AllianceBernstein L.P. v. Atha*, 954 N.Y.S.2d 44 (1st Dept. 2012), the court rejected a request for turnover to the other side and instead ordered the phone to be turned over to the court for an in camera review. In contrast, in *Contra Freres v. Xyngular Corp*., (D. Utah March 31, 2014), the court authorized the copying of a smartphone where a protective order provided a vehicle to address the privacy concerns. And, in *Robinson v. Jones Lang LaSalle Americas* (D. Oregon Aug. 29, 2012), the court placed the burden on counsel "to determine what information falls within the scope of [the] court's order in good faith and consistent with their obligations as officers of the court."

While these issues are complicated, the headlines make clear they are not going away. For example, the Justice Department and Apple recently fought over whether Apple needed to provide access to the cellphone of a terrorist who helped carry out the shooting in San Bernardino, California. Likewise, in the "Deflategate Arbitration," the NFL complained about Tom Brady's alleged destruction of his cellphone, which resulted in the loss of 10,000 text

messages. And, if things were not complicated enough, there is software, such as Snapchat, designed to automatically delete text messages shortly after they are sent.

Steps to Follow in Seeking Smartphone Data

So how can you get this data? We recommend following these steps, starting with a less intrusive option and proceeding further only if warranted based on the facts and the actions of your adversary.

(1) Create a record by: (a) showing you requested the data be preserved in the initial litigation hold; (b) requesting relevant data as part of your document demands; and (c) inquiring of witnesses in depositions how they typically communicate and how they communicated on the issues relevant to the case. Along these lines, during the deposition, you should also ask the deponent to show their smartphone and make a record of the steps the deponent took to preserve the smartphone data.

(2) Seek a court order for the production of all relevant data and require your adversary to certify what was done and that all relevant data was produced. In state court, you can rely on the required Certification of Completeness under N.J. Ct. R. 4:18-1(c). (Support this with prior discovery responses, which indicate that the smartphone may well be the sole source of the information because the service provider no longer has retained the specific contents of text messages.)

(3) Seek a court order that requires the adversary's expert to image the relevant data and make the image available to your expert. Use the discovery obtained to date and technological input from your expert to support the reasonable belief that relevant evidence exists on the targeted smartphone, and that there is a substantial risk that the data will be permanently lost (even absent nefarious intent, such as through a device operating system reinstall). Be prepared with a detailed written imaging and data access protocol.

(4) Seek a court order that the data (or the phones themselves) be turned over to the court for an in camera review.

(5) Seek a court order requiring the retention of an independent expert to access the data on the smartphone.

(6) And, lastly, seek a court order that the smartphone be turned over to you. (To obtain this relief, you will likely need to show either: (a) clear prior acts of spoliation, manipulation of evidence, or intentional comingling of private and business data to conceal illicit activity; or (b) abuse by a party of privilege claims.)

Some Tips for Practitioners

Lastly, here are some tips that attorneys should keep in mind in this changing world. First, advise clients to retain text messages, social media accounts and postings. See *Ewald v. Royal Norwegian Embassy*, (D. Minn Nov. 20, 2013) (finding party's "argument that it was unaware of its obligation to produce text messages … unavailing"). For corporate clients, this might also extend to company employees who use their personal devices to conduct business communications. See *In re Pradaxa Prod. Liab. Lit*., (S.D. Ill. Dec. 9, 2013) ("defendants have a duty to ensure that their employees understood" that they were required to preserve business related text messages contained on their smartphones). Be sure to fully understand your client's methods of communicating and, if text and instant messaging were commonly used, much more care should be taken to preserve the data on relevant devices. See *Goldmark v. Mellina*, (N.J. App. Div. June 18, 2012) (upholding trial court's award of sanctions where law firm failed to timely produce electronic documents).

Second, have a basic understanding of technology, social media, the lingo, etc., and keep up with changes as they occur. Some states have added this as a requirement to the Rules of Professional Conduct, and New Jersey continues to look at this issue. All data is not created equal—and, increasingly, new technologies, by design, allow for data to disappear (or be made to disappear) very quickly. You must have a working knowledge of these new technologies to know what questions to ask your clients and adversaries.

Third, consider retaining forensic experts to assist in the discovery process. While they are costly, forensic experts are often essential in securing discovery of data from mobile sources, by both providing technical expertise to retrieve the data and, as noted above, serving as court-sanctioned intermediaries for the collection and review of these personal and privileged data

that adversaries and courts are loath to release.

In conclusion, until New Jersey courts issue decisions that provide greater clarity, to best position your client to find the smoking gun, create a strong record of the likelihood of responsive data and a failure on the part of your adversary to preserve it. Without such a showing, in light of the strong privacy concerns, costs and burden, the court will be hesitant to order a turnover.